银河风云
nROSE 配置手册
交换分册

文档编号：0209_S9600_v8.0_100706

深圳市银河风云网络系统股份有限公司

地址：深圳市科技园北区松坪新西路五号风云大厦

邮编：518057

电话：（0755）83400088

传真：（0755）33630995

客服：800-999-8305

网址：http://www.galaxywind.com

邮箱：customer@galaxywind.com

目录

目录.....i

第 1 章 适用范围.....1

第 2 章 链路聚合控制协议.....1

2.1. 链路聚合控制协议.....1

2.1.1. lacp 简介.....1

2.1.2. lacp 功能.....1

2.1.3. lacpdu 格式.....2

2.1.4. LACP 协议配置任务.....2

第 3 章 端口汇聚.....5

3.1. Trunk.....5

3.1.1. Trunk 简介.....5

3.1.2. Trunk 的特点.....6

3.1.3. Trunk 的应用.....6

3.1.4. Trunk 配置.....7

3.1.5. Trunk 的监控与维护.....9

3.1.6. Trunk 配置举例.....9

第 4 章 VLAN.....10

4.1. VLAN 基本配置.....10

4.1.1. VLAN 简介.....10

4.1.2. VLAN 基本配置.....17

4.1.3. 监控和维护 VLAN.....21

4.1.4. VLAN 典型配置实例.....22

4.2. VLAN 间路由.....25

4.2.1. VLAN 间路由简介.....25

4.2.2. VLAN 间路由配置.....25

4.2.3. VLAN 间路由配置实例.....26

4.3. Super VLAN.....28

4.3.1. Super VLAN 概述.....28

4.3.2. Super VLAN 配置.....29

4.3.3. Super VLAN 示例.....31

第 5 章 生成树协议.....32

5.1. 多生成树协议（MSTP）.....32

5.1.1. 概述.....32

5.1.2. 多生成树区域.....32

5.1.3. IST, CST, CIST 和 MSTI.....33

5.1.4. 稳定状态 34
5.1.5. 跳数 34
5.1.6. STP 兼容性 35
5.1.7. BPDU 的格式 35
5.2. 生成树协议的配置任务 36
5.2.1. MSTP 配置 37
5.3. MSTP 配置实例 47
5.3.1. 组网需求 47
5.3.2. 组网图 47
5.3.3. 组网配置 47

第 6 章 MSTP 安全防护 49

6.1. MSTP 安全防护 49
6.1.1. Mstp Bpdu Guard 简介 49
6.1.2. Mstp Loop Guard 简介 49
6.1.3. Mstp Root Guard 简介 49
6.1.4. Mstp Bpdu Filter 简介 50
6.1.5. Mstp Bpdu Skewing 简介 50
6.1.6. Mstp Tc Guard 简介 50
6.1.7. MSTP 安全防护配置 51

第 7 章 安全防护 54

7.1. DHCP snooping 54
7.1.1. dhcp snoop 简介 54
7.1.2. dhcp snoop 配置 54
7.2. DHCPv6 snooping 55
7.2.1. dhcpv6 snoop 简介 55
7.2.2. ipv6 dhcp snooping 配置 56

第 8 章 MAC 配置 58

8.1. MAC 配置简介 58
8.2. MAC 的配置任务 58
8.2.1. MAC 的基本配置 58
8.2.2. 监控和维护 MAC 配置 59

第 9 章 交换机控制 61

9.1. 风暴控制 61
9.1.1. 风暴控制简介 61
9.1.2. 风暴控制的配置任务 61
9.2. MAC ACL 63
9.2.1. MAC ACL 简介 63
9.2.2. MAC ACL 的配置 64
9.3. 端口镜像 67
9.3.1. 端口镜像简介 67
9.3.2. 端口镜像的配置 68

第 10 章 PVLAN.....71

10.1. PVLAN (Primary-VLAN).....71
10.1.1. PVLAN 概述.....71
10.1.2. PVLAN 配置.....71
10.1.3. PVLAN 配置实例.....72

第 11 章 802.1x.....74

11.1. 802.1x.....74
11.1.1. 802.1x 简介.....74
11.1.2. 802.1x 配置.....75
11.1.3. 802.1x 的监控与维护.....78
11.1.4. Radius-sever 配置.....78
11.1.5. 802.1x 配置举例.....79
11.2. 配置 802.1x 的 keepalive 功能.....79
11.2.1. 开启/关闭接口 802.1x keepalive 功能.....79
11.2.2. 配置发送 keepalive 间隔时间.....79
11.2.3. 配置 keepalive 超时重传次数.....80
11.3. 802.1x accounting update 功能.....80
11.3.1. 开启/关闭接口 802.1x 计费 update 功能.....80
11.3.2. 配置发送计费 update 间隔时间.....80
11.3.3. 配置计费 update 超时重传次数.....81
11.4. 802.1X 新增特性.....81
11.4.1. 自动注销.....81
11.4.2. 802.1x 的 log.....82

第 12 章 Rmon.....83

12.1. rmon.....83
12.1.1. RMON 概述.....83
12.1.2. RMON 配置.....84

第 13 章 动态 ARP 检查.....87

13.1. 动态 ARP 检查简介.....87
13.2. 动态 ARP 检查（DAI）的配置.....87
13.2.1. 配置 ip 与 mac 绑定关系.....87
13.2.2. 端口使能 DAI 功能.....87
13.2.3. 使能 arp 表自动绑定功能.....88
13.2.4. 使能 arp 冲突检测功能.....88
13.2.5. 转移冲突 arp 信息到 dai 表里.....88
13.2.6. 删除 arp 绑定信息.....89
13.2.7. 显示 dai 信息.....89

第 14 章 邻居发现检测.....90

14.1. ND SNOOP 简介.....90
14.2. ND SNOOP 的配置.....90

14.2.1. 使能 ND SNOOP....90
14.2.2. 配置 ipv6 地址与 mac 绑定关系....90
14.2.3. 显示 nd-snoop 信息....91

第 15 章 环回检测....92

15.1. Loopdetection 简介....92
15.2. Loopdetection 配置....92
15.2.1. 使能 loopdetection....92
15.2.2. loopdetection keepalive....92
15.2.3. Loopdetection 可控制 shutdown....93
15.2.4. Loopdetection 消息老化时间....93
15.2.5. loopdetection 的监控与维护....93

第 16 章 IP、MAC 绑定....96

16.1. Ip mac bind 简介....96
16.2. Ip mac bind 配置....96
16.2.1. 使能/关闭 ip mac bind....96
16.2.2. 配置 ip mac bind 关系....96
16.2.3. 查看 ip mac bind 关系及状态....97

第 1 章 适用范围

适用范围：本分册中包含的命令默认情况下路由，安全，三层交换这三个平台下的各系列机器均支持，如果有系列不支持该命令或者参数有差异，会在【适用范围】中详细说明。

第 2 章 链路聚合控制协议

2.1. 链路聚合控制协议

2.1.1.lacp 简介

链路聚合控制协议(Link Aggregation Control Protocol, LACP)是 IEEE802.3ad 标准的主要内容之一，定义了一种标准的链路聚合控制方式。聚合的双方通过协议交互聚合信息，根据双方的参数和状态，自动将匹配的链路聚合在一起收发数据，依此来提供更高的带宽，防止链路发生故障。

LACP 协议通过 LACPDU（Link Aggregation ControlProtocol Data Unit，链路聚合控制协议数据单元）与对端交互信息。当全局 lacp 协议 enable 后，处于动态聚合组中的接口会自动使能 LACP 协议，该接口将通过发送 LACPDU 向对端通告自己的系统 LACP 协议优先级、系统 MAC、端口的 LACP 协议优先级、端口号和操作 Key。对端接收到 LACPDU 后，将其中的信息与其它接口所收到的信息进行比较，以选择能够处于 Selected 状态的接口，从而双方可以对接口处于 Selected 状态达成一致。

2.1.2.lacp 功能

1. 增加带宽：在带宽比较紧张的情况下，可以通过逻辑聚合链路扩展带宽到原单一链路的 n 倍

2. 增加实用型：链路聚合中，成员互相动态备份，当一个链路组中某一条单独链路出现故障，其它链路成员能够迅速接替其工作。启用备份过程只在聚合链路内，与其它链路无关，切换可在数毫秒内完成。

3. 负载分担：聚合模块按照一定算法将业务流量分配给不同的成员，实现链路级的负载分担功能。

4. 自动配置：在不考虑手动配置的情况下，根据双方的参数和状态，自动将匹配的链路聚合在一起配置成链路组来收发数据。如果一条链路可以被汇聚，它将被汇聚到该链路组。

5. 快速配置及重新配置：聚合形成后，交换设备维护聚合链路状态，当物理连通性改变时，链路汇聚会重新聚合（自动调整或解散聚合链路）成新的配置，该配置过程可以在 1 秒或者更短时间内完成。

2.1.3.lacpdu 格式

值域	字节位	占有字节
Destination Address	1~6	6
Source Address	7~12	6
Length/Type	13~14	2
Subtype = LACP	15	1
Version Number	16	1
TLV_type = Actor Information	17	1
Actor_Information_Length = 20	18	1
Actor_System_Priority	19~20	2
Actor_System	21~26	6
Actor_Key	27~28	2
Actor_Port_Priority	29~30	2
Actor_Port	31~32	2
Actor_State	33	1
Reserved	34~36	3
TLV_type = Partner Information	37	1
Partner_Information_Length = 20	38	1
Partner_System_Priority	39~40	2
Partner_System	41~46	6
Partner_Key	47~48	2
Partner_Port_Priority	49~50	2
Partner_Port	51~52	2
Partner_State	53	1
Reserved	54~56	3
TLV_type = Collector Information	57	1
Collector_Information_Length = 16	58	1
CollectorMaxDelay	59~60	2
Reserved	61~72	12
TLV_type = Terminator	73	1
Terminator_Length = 0	74	1
Reserved	75~124	50
FCS	125~128	4

2.1.4.LACP 协议配置任务

在 lacp 协议启动后才能配置 lacp 动态聚合组及其成员，也只有在 LACP 启动后这些配置才会生效，完成链路聚合。同样查看 lacp 聚合组信息也只有在 lacp 全局启动后才能进行。

2.1.4.1. LACP 配置

1. 开启设备的 LACP 协议

该命令用来开启设备的 LACP 协议。

表 2-1 开启设备或接口上的 LACP 协议

命令	命令模式	功能说明
lacp{ enable | disable }	全局配置模式	开启/关闭设备的 LACP 协议。

参数说明：

enable：用来开启设备的 LACP 协议。

disable：用来关闭设备的 LACP 协议。

以太网交换机启用 LACP 后，如果未配置 lacp 聚合组，则默认为没有 lacp 聚合组。

设备启动了 LACP 协议后，开始配置聚合组成员并运行 lacp。

【示例】开启设备的 MSTP 协议。

Tritium(config)# lacp **enable**

2. 配置 lacp 聚合组

该命令用来配置 lacp 聚合组及其成员

表 2-2 配置 lacp 聚合组及成员

命令	命令模式	功能说明
Lacp group-id *group-id* port *slot-list/port-list*	全局配置模式	配置 lacp 聚合组 并加入成员。
no group-id *group-id*	全局配置模式	删除 lacp 聚合组

参数说明：

group-id ： lacp 聚合组 ID。
slot-list： 加入 lacp 聚合组的板子的号
port-list：加入 lacp 聚合组的 port，slot/port 之间通过“,”连接

设备启动了 LACP 协议，才可以配置动态聚合组，关闭 LACP 协议后，聚合组成员停止运行协议，并从聚合组中解聚合出来，同时所有 lacp 聚合组会被清除。

【示例】配置设备的 lacp 聚合组并加入成员。

Tritium(config)# lacp group-id *5* **port** *1/2,1/3, 1/8*

删除一个汇聚组。

Tritium(config)# no lacp group-id *5*

3. 删除配置 lacp 聚合组中成员或者删除一个 lacp 聚合组

该命令用来删除 lacp 聚合组或其成员

表 2-3 配置 lacp 聚合组及成员

命令	命令模式	功能说明
No lacp group-id *group-id* port *slot-list/port-list*	全局配置模式	删除 lacp 聚合组中成员
no group-id *group-id*	全局配置模式	删除 lacp 聚合组

参数说明：

group-id ： lacp 聚合组 ID。
slot-list： 加入 lacp 聚合组的板子的号
port-list：要删除的 lacp 聚合组中的 port，slot/port 之间通过“,”连接

【示例】删除设备的 lacp 聚合组成员。

Tritium(config)# no **lacp group-id** *5* **port** *1/2,1/3*
删除一个汇聚组。

Tritium(config)# no lacp group-id *5*

2.1.4.2. 查看 LACP 聚合组信息

该命令用来显示各 lacp 聚合组信息

表 2-4 查看 LACP 聚合组信息

命令	命令模式	功能说明
show lacp { group-id *group-id* | all}	特权用户模式	查看 LACP 聚合组信息

参数说明：

group-id：lacp 聚合组 ID，

all：查看所有 lacp 聚合组信息
必须在配置 lacp 协议全局 enable 后才能查看 lacp 聚合组信息。

【示例】显示某 lacp 聚合组的成员信息

Tritium# show lacp group-id *5*

第 3 章 端口汇聚

3.1. Trunk

3.1.1. Trunk 简介

Trunk 是端口汇聚的意思，就是通过软件配置，将两个或多个物理端口组合在一起成为一条逻辑的路径从而增加在交换机和网络节点之间的带宽，通过几个端口的带宽合并，给端口提供一个几倍于独立端口的独享的高带宽。以实现出入负荷在各成员端口中的分担，同时也提供了更高的连接可靠性。Trunk 是一种封装技术，它是一条点到点的链路。

一般情况下，在没有使用 Trunk 时，百兆以太网的双绞线的这种传输介质特性决定在两个互连的普通 10/100 交换机的带宽仅为 100M，如果是采用的全双工模式的话，则传输的最大带宽可以达到最大 200M，这样就形成了网络主干和服务器瓶颈。要达到更高的数据传输率，则需要更换传输媒介，使用千兆光纤或升级成为千兆以太网，这样虽能在带宽上能够达到千兆，但成本却非常昂贵（可能连交换机也需要一块换掉）。如果使用 Trunk 技术，把四个端口通过捆绑在一起来达到 800M 带宽，这样可较好的解决了成本和性能的矛盾。

端口汇聚（Trunk）功能，允许交换机与交换机、交换机与路由器、主机与交换机或路由器之间通过两个或多个端口并行连接同时传输以提供更高带宽、更大吞吐量，大幅度提供整个网络能力。

同一个汇聚组中端口的基本配置应该保持一致，即如果某端口为 Trunk 端口，则其他端口也配置为 Trunk 端口。

千兆百兆均可以随意聚合，而且支持跨板聚合，也就是说配置的灵活性也是非常的大。

当然，千兆百兆的聚合这种情况，并不会出现千兆走一半数据百兆走另一半，这样的话也不符合 Trunk 的功能要求，实际上这种聚合情况，是通过速率自动算出从千兆走的可能性更大，从百兆走的可能性更小，换句话说，如果 100 个数据包，从一个千兆一个百兆聚合的 Trunk 发送，从千兆口发出的几率是 90%，从十兆口发送的几率是 10%。这样也会有效地增加实际速率的利用率。

3.1.2.Trunk 的特点

风云 Tritium S 系列交换机，除了实现上的灵活性以外，更有配置上的智能性特点，用户只需要几条简单的配置命令，就能使用其强大的功能，这也是我们整个产品所共有的特点。

1、可以在 VLAN 成员添加的配置里面像添加 port 一样直接添加任意 Trunk 组作为其成员，非常方便。

2、Trunk 组也可以像配置 port 一样，配置 pvid，IP Trunk 配置 IP 等。

3、交换 Trunk 同样支持生成树，新建立或者转换的交换 Trunk 都会自动加入生成树中，由于 Trunk 本来就是用于点到点的连接，因此在生成树中不需用户手工配置，缺省加入的 Trunk 组就是 P2P 的。Port 能够进行的生成树相关配置，同样也能在 Trunk 下面配置。

3.1.3.Trunk 的应用

Trunk（端口汇聚）是在交换机和网络设备之间比较经济的增加带宽的方法，如服务器、路由器、工作站或其他交换机。这中增加带宽的方法在当单一交换机和节点之间连接不能满足负荷时是比较有效的。

Trunk 的主要功能就是将多个物理端口绑定为一个逻辑的通道，使其工作起来就像一个通道一样。将多个物理链路捆绑在一起后，不但提升了整个网络的带宽，而且数据还可以同时经由被绑定的多个物理链路传输，具有链路冗余的作用，在网络出现故障或其他原因断开其中一条或多条链路时，剩下的链路还可以工作。

Trunk 功能比较适合于以下方面具体应用：

1、Trunk 功能用于与服务器相联，给服务器提供独享的高带宽。

2、Trunk 功能用于交换机之间的级联，通过牺牲端口数来给交换机之间的数据交换提供捆绑的高带宽，提高网络速度，突破网络瓶颈，进而大幅提高网络性能。

3、Trunk 可以提供负载均衡能力以及系统容错。由于 Trunk 实时平衡各个交换机端口和服务器接口的流量，一旦某个端口出现故障，它会自动把故障端口从 Trunk 组中撤消，进而重新分配各个 Trunk 端口的流量，从而实现系统容错。

3.1.4. Trunk 配置

3.1.4.1. 建立端口汇聚组

新建立的 Trunk 是一个没有成员的接口，必须要添加接口以后才能使用，L2 Trunk 缺省情况下属于 VLAN 1。缺省情况下没有任何汇聚组。。

表 3–1 建立端口汇聚组

命令	命令模式	功能说明
port-trunk *group-id*	全局配置模式	建立端口汇聚组并进入 Trunk 接口配置模式。
no port-trunk *group-id*	全局配置模式	删除某个端口汇聚组。

【适用范围】

三层交换 S8508 系列：

trunk-group-id：范围为 1-30。

3.1.4.2. 配置汇聚组中的端口

三层交换 S8508 系列每个 Trunk 组不能超过 8 个端口。

表 3–2 配置汇聚组中的端口

命令	命令模式	功能说明
port *slot-list/port-list*	port-trunk 手工配置模式	配置聚合组中的端口，添加一个端口或端口列表到聚合组。
no port *slot-list/port-list*	port-trunk 手工配置模式	从聚合组删除一个端口或端口列表。

3.1.4.3. 进入 port-trunk 的接口配置模式

表 3–3 进入 port-trunk 的接口配置模式

命令	命令模式	功能说明
interface port-trunk { *trunk-group-id* }	全局配置模式	进入 port-trunk 的接口配置模式。

【适用范围】

三层交换 S8508 系列：

trunk-group-id：范围为 1-30

3.1.4.4. 配置汇聚组描述信息

表 3–4 配置汇聚组描述信息

命令	命令模式	功能说明
description *string*	port-trunk 接口配置模式	配置聚合组描述信息。
no description	port-trunk 接口配置模式	删除聚合组描述信息。

3.1.4.5. 配置 port-trunk 负载均衡方式

该命令用于配置 port-trunk 的负载均衡算法。

表 3–5 配置 port-trunk 负载均衡方式

命令	命令模式	功能说明
load-balance {*dst-ip*| *src-dst-ip*| *src-dst-mac*| *src-ip*|*src-mac*}	port-trunk 配置模式	设置均衡算法。
no load-balance	port-trunk 配置模式	恢复均衡算法缺省值 src-mac。

参数说明：

dst-ip：以目的 ip 负载均衡

src-dst-ip ： 以目的和源 ip 负载均衡

src-dst-mac ： 以目的和源 mac 负载均衡

src-ip ： 以源 ip 负载均衡

src-mac ： 以源 mac 负载均衡

no ： 恢复到缺省状态，src-mac

【示例 1】配置 port-trunk 1 为以目的和源 mac 的负载均衡。

Tritium(config)# port-trunk *1*

Tritium(config-trunk)# load-balance *src-dst-mac*

3.1.5.Trunk 的监控与维护

表 3–6 Trunk 的监控与维护

命令	命令模式	功能说明
debug switch port-trunk	特权用户模式	调试 port-trunk 功能。
no debug switch port-trunk	特权用户模式	关闭 debug 模式。
show port-trunk { *trunk-group-id* | **all** }	特权用户模式	打印聚合组中的端口信息。

【适用范围】

三层交换 S8508 系列：

trunk-group-id：范围为 1-30。

3.1.6.Trunk 配置举例

建立端口 GigabitEthernet 1/1，1/2，1/3 的聚合配置。

！建立聚合组，组号 1

Tritium# config

Tritium(config)# port-trunk *1*

！加入端口 1/1~1/4 到这个聚合组

Tritium(config-trunk)# port *1/1,1/2,1/3,1/4*

！从这个聚合组删除端口 1/4

Tritium(config-trunk)# no port *1/4*

Tritium(config-trunk)# exit

Tritium(config)# exit

！打印聚合组信息

Tritium# show port-trunk all

Trunk ID: 1
Member Ports:
1/1,1/2,1/3

第 4 章 VLAN

4.1. VLAN 基本配置

4.1.1.VLAN 简介

VLAN（Virtual Local Area Network）即虚拟局域网，是指通过将位于一个或多个局域网内设备的逻辑地址而不是物理地址划分成一个个网段从而实现虚拟工作组。由于 VLAN 基于逻辑连接而不是物理连接，所以它可以提供灵活的用户、主机管理，带宽分配以及资源优化等服务。IEEE 于 2003 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议的最新标准。

4.1.1.1. VLAN 基础

1. 什么是 VLAN

VLAN 是在 LAN（Local Area Network，局域网）的发展基础上产生的，所以在介绍 VLAN 之前，我们先来了解一下局域网的有关知识。

起初，LAN 被定义为：由一些处于同一物理空间范围内的计算机组成的网络，计算机之间通过集线器（Hub）或中继器（Repeater）相连接。如果有两台或两台以上计算机同时想要通过 LAN 的通信总线发送数据时，它们将发生冲突，已发送的数据就会丢失。再者，一旦有冲突发生，冲突将通过集线器或中继器被传送到整个网络中，使得暂时谁也无法再发送数据。于是发送者们只好停下来，等到这次冲突平息之后再试着去发送已丢失的数据——这是对时间和资源的很大浪费。

为了防止冲突被发送给 LAN 中的每一台计算机，人们使用了网桥（Bridge）或局域网交换机来隔离冲突——网桥和交换机都不会转发冲突，但它们会让广播报文或多播报文通过。这样，原来的一个 LAN 就被网桥和交换机分隔成了多个 LAN 网段。另一方面，人们使用路由器来隔离广播，防止广播或多播报文被转发到另一个网络中去。被路由器这样隔离开来的一个个网络被称为广播域。VLAN 所指的 LAN 特指使用路由器分割的网络——通常是一个单独的广播域。下图所示即为使用路由器构建的典型的局域网环境。

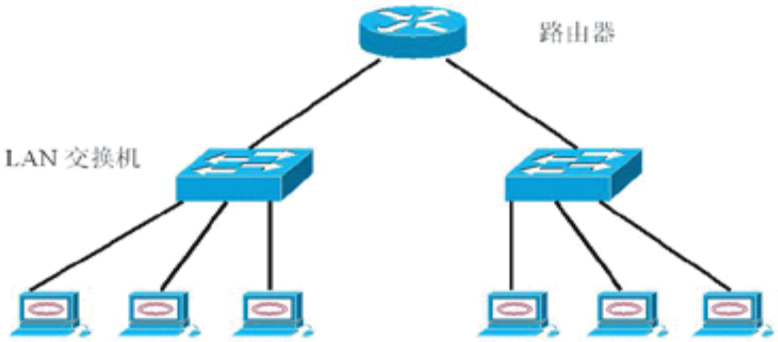


图 4–1 传统的 LAN 环境

随着网络的不断扩展，接入设备逐渐增多，网络结构也日趋复杂，必须使用更多的路由器才能将不同的用户划分到各自的广播域中，在不同的局域网之间提供网络互联。

但这样做会存在两个缺陷：

首先，随着网络中路由器数量的增多，网络时延逐渐加长，从而导致网络数据传输速度的下降。这主要是因为数据在从一个局域网传递到另一个局域网时，必须经过路由器的路由操作：路由器根据数据包中的相应信息确定数据包的目标地址，然后再选择合适的路径转发出去。

其次，传统的 LAN 用户是按照它们的物理连接被自然地划分到不同的用户组（广播域）中。这种分割方式并不是根据工作组中所有用户的共同需要和带宽的需求来进行的。因此，尽管不同的工作组或部门对带宽的需求有很大的差异，但它们却被机械地划分到同一个广播域中。每一个局域网上的广播数据包都可以被该段上的所有设备收到，而无论这些设备是否需要。一方面广播信息消耗了网络整体的带宽，另一方面，收到广播信息的计算机还要消耗一部分 CPU 时间来对它进行处理。造成了网络带宽和 CPU 运算能力的大量无谓消耗。

随着现代企业中跨部门跨职能的开发团队出现得越来越多，企业内部对于灵活、动态地组建 LAN 网段的要求也越来越多。更重要的是，企业的财务部门需要越来越高的安全性，不能和其他的部门混用一个以太网段，以防止数据窃听。所以，客观上要求 LAN 本身的结构可以实现动态组建、调整和管理。这时，虚拟局域网技术，就适时地出现了。

VLAN 是根据逻辑地址划分的一组设备和用户，这些设备和用户并不受物理网段的限制（即不一定被放置在同一个物理空间里），可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。

2. 组建 VLAN 的条件

VLAN 是建立在物理网络基础上的一种逻辑子网，因此建立 VLAN 需要相应的支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，需要路由的支持，这时就可采用具有路由功能的三层交换机来完成。

4.1.1.2. VLAN 的优点

VLAN 是一种比较新的技术，工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于提高网络性能、组建虚拟组织、简化网络管理、提高网络安全等。

1. 提高网络性能

应用 VLAN 技术可以提高网络性能，控制广播风暴：

其一，VLAN 技术允许网络管理者将交换机上的端口作逻辑分组，使得从某个 VLAN 中产生的字节流只能在从属于该 VLAN 的交换机端口之间流动。在一个有大量广播和多播报文的网络中，应用 VLAN 技术可以把这些报文限制在各个 VLAN 里，从而可以大大减少整个网络中不必要的信息流量，一定程度上控制了广播风暴，提高了网络性能。

其二，相比较网桥和交换机而言，路由器在处理接收到的数据时要慢一些。使用了 VLAN 技术后，三层交换机集路由与交换于一身，在交换机内部实现了路由， 人们可以用交换机来代替路由器隔离广播域，提高了网络的整体性能。

2. 组建虚拟组织

VLAN 技术是随着人们生产活动中越来越多的跨部门跨职能开发团队的出现而提出的。组建虚拟组织、特别是虚拟工作组、是提出 VLAN 技术的初衷和目标之一。在实际应用时，对于同一个工作组内的成员，在该工作组存在的短时期内，可以把他们的计算机工作站划分在一个 VLAN 里以便与其进行通信。这样，每个组内成员的计算机工作站既无需搬移到一起、也无需改变各自的设置，只需在网络管理者那里做一些改变就可以了。

3. 简化网络管理

根据 David J.Buerger 的分析计算，传统的 LAN 中约有 70%的网络花销是因为添加、删除、移动、更改网络用户而导致的。每当有一个用户加入局域网，就会因此而引发一系列的

端口分配、地址分配、网络设备重新配置等网络管理任务。然而在使用 VLAN 技术后，这些任务都可得以简化。举例来说，当某一部门物理位置发生变化时，只需对交换机进行设置，就可以实现网络的重组，非常方便、快捷，同时节约了成本。

4. 提高网络安全

在以往的局域网中，不时的会有些敏感数据被有意或无意地广播到网络上，从而有可能造成信息泄密。在这种情况下，确定谁可以访问到这些数据就显得很重要。使用 VLAN 技术可以将敏感数据的传播限制在安全范围内，只允许已定义的 VLAN 成员访问相关数据。VLAN 还可被用来设立防火墙、限制数据访问以及将网络入侵事件通知给网络管理者等，这些都可以提高网络的安全系数。

4.1.1.3. VLAN 的划分

VLAN 的划分最简单、最有效的方式是基于端口来划分。基于端口的 VLAN 划分是以网络设备的哪个端口属于哪个 VLAN 的标准来划分 VLAN 的。VLAN 从逻辑上把局域网交换机的端口划分开来，从而把终端系统划分为不同的部分，各部分相对独立，在功能上模拟了传统的局域网。基于端口的 VLAN 又分为单交换机端口和多交换机端口定义 VLAN 两种情况：

1. 单交换机端口定义 VLAN

如图 2-2 所示，在一个有 8 个端口的网桥中，端口 1、2、6、7、8 属于 VLAN1，而端口 3、4、5 属于 VLAN2。则与这些端口相连的设备这些设备、收发的数据帧相应地也分别属于 VLAN1、VLAN2。

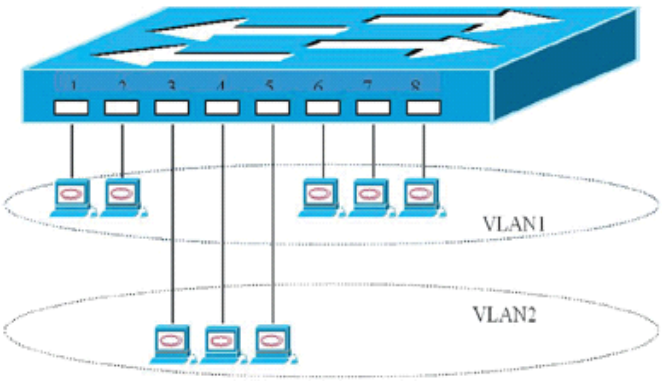


图 4–2 单交换机端口定义 VLAN

2. 多交换机端口定义 VLAN

如果有多个网络设备的话，如图 2-3 所示，则可以指定交换机 1 的 1、2、3 端口和交换机 2 的 4、5、6 端口组成 VLAN1，交换机 1 的 4、5、6、7、8 端口和交换机 2 的 1、2、3、7、8 端口组成 VLAN2，即同一 VLAN 可以跨越数个交换机。

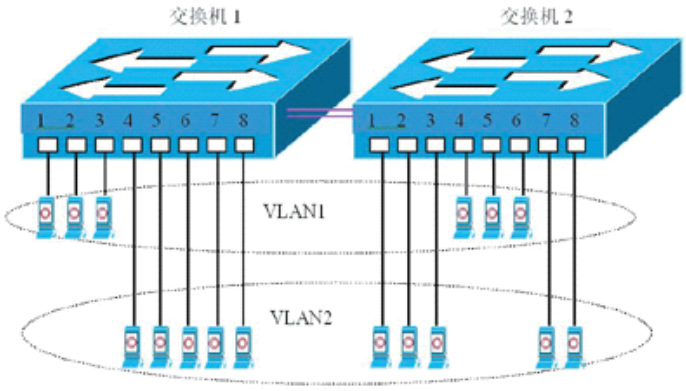


图 4–3 多交换机端口定义 VLAN

根据端口划分是目前定义 VLAN 的最常用的方法，IEEE 802.1Q 协议标准草案中对如何根据交换机的端口来划分 VLAN 给出了明确的规定。这种划分方法的优点和缺点都很明显：优点是定义 VLAN 成员时非常简单，只要将所有的端口都指定一下就可以了，不用考虑该端口所连接的设备；缺点是不允许用户随便移动，如果属于某个 VLAN 的用户离开了原来的端口，到了一个新的网络设备的某个端口，那么网络管理者就必须重新定义 VLAN。

4.1.1.4. VLAN 的实现

当一个交换机接收到来自于某个工作站的数据帧，它将给这个数据帧加上一个标签以标识这个数据帧来自于哪个 VLAN。交换机都有一个不断升级更新的数据库，这个数据库叫做过滤数据库，包含了本网络中全部 VLAN 之间的映射以及它们使用哪个字段作为标签。

基于 IEEE 802.1Q 协议时，4 个字节的 VLAN 标签被加到传统的以太网帧的目的 MAC 地址字段和协议类型字段（在符合 IEEE 802.3 协议的帧中是长度字段）之间。其中包含有一个 12 比特大小的 VLAN ID 号以区别各个 VLAN。

图 4–4 基于 802.1Q 协议的 VLAN 帧格式封装类型

由于 802.1Q 协议的标签头的 4 个字节是新增加的，故目前使用的计算机并不支持 802.1Q，即计算机发送出去的数据包的以太网帧头还不包含这 4 个字节，同时也无法识别这

4 个字节。对于交换机来说，如果它所连接的以太网段的所有主机都能识别和发送这种带 802.1Q 标签头的数据包，该端口称为 Tag Aware 端口，则需要给数据帧加标签：相反，如果该交换机端口所连接的以太网段里只要有一台主机不支持这种带 802.1Q 标签头的数据包，该端口称为 Access 端口，则不能给数据帧加标签。

对于每一个到来的 VLAN 帧，交换机将根据查找过滤数据库的结果决定该帧归属于哪一个 VLAN、将从哪个接口被转发出去。一旦交换机决定了某个数据帧的下一步去向，它就得决定是否需要给这个数据帧加标签。

具体实现包括以下三个过程：

（1） 接收过程：该过程负责接收数据包，数据包可以是带标签头的，也可以不带标签头，如果不带，交换机会知道根据该端口的 PVID 添加上相应的标签头。

（2） 查找过滤数据库过程：该过程根据数据包的目的 MAC 地址、VLAN 标识，查找过滤数据库中注册的信息，以决定把数据包发送到哪个端口。

（3） 发送过程：将数据包发送到以太网段上，如果该网段的主机不能识别 802.1Q 标签头，则将该标签头去掉；如果是发送到互连的其他交换机的端口，则标签头一般不去掉。

4.1.1.5. VLAN 的应用

由于虚拟局域网具有比较明显的优势，在各种企业中都有了很好的应用。

1. 局域网内部的局域网

往往很多企业已经具有一个相当规模的局域网，但是现在企业内部因为保密或者其他原因，要求各业务部门或者课题组独立成为一个局域网，同时，各业务部门或者课题组的人员不一定是在同一个办公地点，各网络之间不允许互相访问。根据这种情况，可以有几种解决方法，但是虚拟局域网解决方法可能是最好的。为了完成上述任务，我们要做的工作是收集各部门或者课题组的人员组成、所在位置、与交换机连接的端口等信息。根据部门数量对交换机进行配置，创建虚拟局域网，配置中继，最后，在一个公用的局域网内部划分出来若干个虚拟的局域网，同时减少了局域网内的广播，提高了网络传输性能。这样的虚拟局域网可以方便地根据需要增加、改变、删除。

2. 共享访问——访问共同的接入点和服务器

在一些大型写字楼或商业建筑（酒店、展览中心等），经常存在这样的现象：大楼出租

给各个单位，并且大楼内部已经构建好了局域网，提供给入驻企业或客户网络平台，并通过共同的出口访问 Internet 或者大楼内部的综合信息服务器。由于大楼的网络平台是统一的，使用的客户有物业管理人员、有其他不同单位的客户。在这样一个共享的网络环境下，解决不同企业或单位对网络的需求的同时，还要保证各企业间信息的独立性。这种情况下，虚拟局域网提供了很好的解决方案。大厦的系统管理员可以为入驻企业创建一个个独立的虚拟局域网，保证企业内部的互相访问和企业间信息的独立，然后利用中继技术，将提供接入服务的代理服务器或者路由器所对应的局域网接口配置成为中继模式，实现共享接入。这种配置方式还有一个好处，可以根据需要设置中继的访问许可，灵活地允许或者拒绝某个虚拟局域网的访问。

3. 交叠虚拟局域网

交叠虚拟局域网是在基于端口划分虚拟局域网的基础上提出来的，最早的交换机每一个端口只能同时属于一个虚拟局域网，交叠虚拟局域网允许一个交换机端口同时属于多个虚拟局域网。这种技术可以解决一些突发性的、临时性的虚拟局域网划分。比如在一个科研机构，已经划分了若干个虚拟局域网，但是因为某个科研任务，从各个虚拟局域网里面抽调出来技术人员临时组成课题组，要求课题组内部通信自如，同时各科研人员还要保持和原来的虚拟局域网进行信息交流。如果采用路由和访问列表控制技术，成本会较大，同时会降低网络性能。交叠技术的出现，为这一问题提供了廉价的解决方法；只需要将要加入课题组的人员所对应的交换机端口设置成为支持多个虚拟局域网，然后创建一个新虚拟局域网，将所有人员划分到新虚拟局域网，保持各人员原来所属虚拟局域网不变即可。

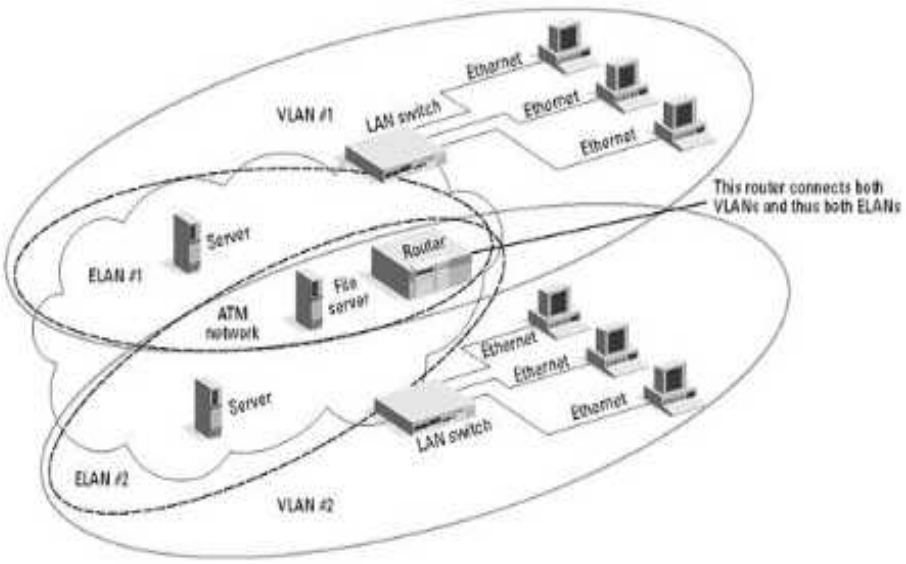


图 4–5 交叠虚拟局域网

随着现代交换技术的发展而出现，并将随着网络的应用得到普及，虚拟局域网将成为众多网络设计、规划和管理人员欢迎和使用的技术。

4.1.2.VLAN 基本配置

4.1.2.1. 创建/删除 VLAN

该命令用于创建某个 VLAN，并进入 VLAN 配置模式。**no** 命令删除某个 VLAN。

表 4–6 创建 VLAN

命令	命令模式	功能说明
vlan *vlan-id* [**name** *vlan-name*]	全局配置模式	创建 VLAN 并进入 VLAN 配置模式。
no vlan *vlan-id*	全局配置模式	删除某个 VLAN。
vlan *vlan-id* **name**	全局配置模式	删除某个 VLAN 的名字。

参数说明：

vlan-id：该 VLAN 的 ID。（1~4094）。

vlan-name：该 VLAN 的名字。（字符串长度为 1~14）。

【示例】创建 VLAN 100 并进入 VLAN 配置模式。

Tritium(config)# vlan *100*

Tritium(config-vlan)#

4.1.2.2. 添加/删除成员的端口

该命令用于为该 VLAN 添加或删除成员的端口。缺省情况下为 **tagged**。

表 4–7 添加成员的端口

命令	命令模式	功能说明
port *slot/port-list* [**tagged** | **untagged**]	VLAN 配置模式	为该 VLAN 添加成员的端口。
no port *slot/port-list*	VLAN 配置模式	删除成员端口。

参数说明：

slot：加入 VLAN 的板子的 slot 号。

port-list：加入 VLAN 的 port 的集合，通过“,”或“-”连接。

【示例】下面的命令将添加 ID 为 30 的 VLAN，GigabitEthernet 1/1、1/3、1/6、1/7、1/8

加入 VLAN 30。

Tritium(config)# vlan *30*

Tritium(config-vlan)# port *1/1,3,6-8*

4.1.2.3. 添加/删除 Trunk 成员的端口

该命令用于为该 VLAN 添加或删除 Trunk 成员的端口。缺省情况下为 tagged。

表 4–8 添加成员的端口

命令	命令模式	功能说明
trunk *trunk-id* { **tagged** | **untagged** }	VLAN 配置模式	为该 VLAN 添加 Trunk 成员的端口。
no trunk *trunk-id*	VLAN 配置模式	删除 Trunk 成员端口。

4.1.2.4. 指定接口是否属于某些 VLAN

该命令用于指定该接口是否属于某些 VLAN。缺省情况下为 **tagged**。

表 4–9 指定该接口属于某/些 VLAN

命令	命令模式	功能说明
switchport access { **vlan** *vlan-id-list* | **name** *vlan-name-list* } { **tagged** | **untagged** }	以太网接口配置模式 potr-trunk 接口配置模式	指定该接口属于某些 VLAN。
no switchport access { **vlan** *vlan-id-list* | **name** *vlan-name-list* }	以太网接口配置模式 potr-trunk 接口配置模式	指定该接口不属于某些 VLAN。

参数说明：

vlan-id-list：此接口所属于的 VLAN 的 ID 号，通过“,”或“-”连接。

vlan-name-list：此接口所属于的 VLAN 的名字，通过","连接。

【示例】将当前接口加入 VLAN 2,5,7。

Tritium(config-if)# switchport access vlan *2,5,7*

4.1.2.5. 设置接口是否允许 VLAN 过滤

该命令用于设置该接口是否允许 VLAN 过滤，即是否过滤不属于所属 VLAN 的报文。缺省情况下开启 VLAN 过滤。

表 4–10 设置该接口允许 VLAN 过滤

命令	命令模式	功能说明
switchport vlan-filtering	以太网接口配置模式 potr-trunk 接口配置模式	设置该接口允许 VLAN 过滤，即过滤不属于所属 VLAN 的报文。
no switchport vlan-filtering	以太网接口配置模式 potr-trunk 接口配置模式	禁止 VLAN 过滤，即不过滤不属于 VLAN 的报文。

【示例】允许 VLAN 过滤不属于 VLAN 的报文。

Tritium(config-if)# switchport vlan-filtering

4.1.2.6. 设置接口是否允许接收 untagged 报文

该命令用于设置该接口是否允许接收 untagged 报文。缺省情况下允许接收所有类型的报文。

表 4–11 设置该接口是否允许接收 untagged 报文

命令	命令模式	功能说明
switchport acceptable-frame-types { **all** | **tagged** }	以太网接口配置模式 potr-trunk 接口配置模式	设置该接口允许接收报文。
no switchport acceptable-frame-types	以太网接口配置模式 potr-trunk 接口配置模式	恢复默认配置。

【示例】设置接口只接收 tagged 类型报文。

Tritium(config-if)# switchport acceptable-frame-types tagged

4.1.2.7. 设置接口的 pvid 号

该命令用于设置该接口的 pvid 号（1~4094）。**no** 的时候该接口的 pvid 恢复为初始值 1。缺省 pvid 为 1。如果接口只加入一个 VLAN，那么其 PVID 号和 VLAN 号应相同；如果接口加入多个 VLAN，选其中一个 VLAN 号作为 PVID 号。

表 4–12 设置该接口的 pvid 号

命令	命令模式	功能说明
switchport pvid *pvid*	以太网接口配置模式 potr-trunk 接口配置模式	设置该接口的 pvid 号。
no switchport pvid	以太网接口配置模式 potr-trunk 接口配置模式	该接口的 pvid 恢复为初始值 1。

参数说明：

pvid：此接口的 pvid（1~4094）。

【示例】设置接口的 pvid 为 10。

Tritium(config-if)# switchport pvid *10*

4.1.2.8. 批量创建 vlan

该命令用于批量建立没有 vlan-name 的 vlan。

表 4–13 进入 VLAN 接口配置模式

命令	命令模式	功能说明
Vlan-create { *vlan-idlist* }	全局配置模式	批量建立 vlan。

参数说明：

vlan-id list：格式为 a,b,c 或 a-n。

【示例】批量创建 vlan id 为 2,3,5,100-200 的 vlan。

Tritium(config)# vlan-create *2,3,5,100-200*

4.1.2.9. 批量删除 vlan

该命令用于批量删除 vlan。

表 4–14 进入 VLAN 接口配置模式

命令	命令模式	功能说明
Vlan- destroy { *vlan-idlist* }	全局配置模式	批量删除 vlan。

参数说明：

vlan-id list：格式为 a,b,c 或 a-n。

【示例】批量删除 vlan id 为 2,3,5,100-200 的 vlan。

Tritium(config)# vlan- destroy *2,3,5,100-200*

4.1.2.10. 批量配置接口 pvid

该命令用于批量配置接口 pvid。

表 4–1 批量配置接口 pvid

命令	命令模式	功能说明
vlan-pvid *pvid* **port** *port-list*	全局配置模式	批量配置接口 pvid

no vlan-pvid *pvid* **port** *port-list*	全局配置模式	批量清除接口 pvid

参数说明：

pvid：接口 pvid。

port-list：需要设置接口 pvid 的接口列表。

4.1.3. 监控和维护 VLAN

在完成上述配置后，执行 **debug** 和 **show** 命令可以查看 VLAN 的运行信息，验证配置的效果。

表 4–2 监控和维护 VLAN

命令	命令模式	功能说明
debug switch vlan { **all** | **error** | **trace** }	特权用户模式	显示 VLAN 相关配置的信息。
show vlan { **vlan-id** *vlan-id* | **name** *vlan-name* | **static** | **all** }	特权用户模式	查看已经配置的 VLAN 的配置信息。按 VLAN 排列。
show mac-address { **static** | **dynamic** | **all** } **show mac-address** { **vlan-id** *vlan-id* | **vlan-name** *vlan-name* }	特权用户模式	查看已经配置的 mac-address 信息。
show interfaces vlan { *vlan-id* | *vlan-name* }	特权用户模式	显示 VLAN 接口信息，包括接口状态、IP 地址、掩码、MTU 等。

参数说明：

vlan-id：该 VLAN 的 ID。（1~4094）。

vlan-name：该 VLAN 的名字。（字符串长度为 1~14）。

【示例 1】查看已经配置的所有 VLAN 的配置信息。

```
Tritium# show vlan all
--------------------------------------------------------------------------------
vlan ID: 1 vlan Name: default Type: normal
Member Ports:
3/0-10,13-25
4/0-16,18,20-21,23-25
6/0-25
8/0-25
Untagged Ports:
3/0-10,13-25
4/0-16,18,20-21,23-25
6/0-25
8/0-25
```

Member Trunks:
3
Untagged Trunks:
3
---
vlan ID: 6 vlan Name: Type: normal
Member Ports:
6/6
Untagged Ports:
Member Trunks:
Untagged Trunks:

【示例 2】查看已经配置的所有 MAC 信息。

Tritium# show mac-address all

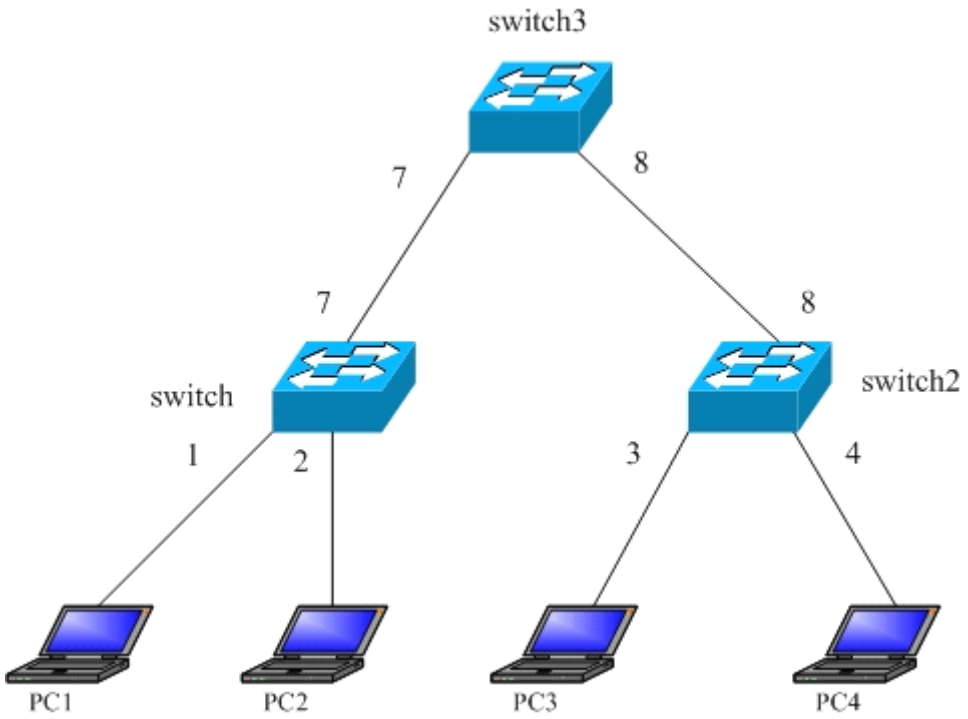
mac age-timer: 600 second
mac count:2
============fwd table============
mac-address dynamic 00:00:00:00:00:29 fastethernet 1/1 vlan-id 1
mac-address static 00:00:00:00:11:22 fastethernet 1/3 vlan-id 2

4.1.4.VLAN 典型配置实例

4.1.4.1. 组网需求

PC1,PC2,PC3 在同一 VLAN,PC4 在另一 VLAN. switch3 作为 PC 网关.

4.1.4.2. 组网图



4.1.4.3. 配置步骤

（1） 配置 switch

！创建 VLAN 11。

Tritium(config)# vlan *11*

！向 VLAN 11 添加端口。

Tritium(config-vlan)# port *1/1,2 untagged*

Tritium(config-vlan)# port *1/7*

Tritium(config-vlan)# exit

！设置 PVID

Tritium(config)# interface gigabitethernet *1/1*

Tritium(config-if)# switchport pvid *11*

Tritium(config)# interface gigabitethernet *1/2*

Tritium(config-if)# switchport pvid *11*

（2） 配置 Switch2

！ 创建 VLAN 11。

Tritium(config)# vlan *11*

！ 向 VLAN 11 添加端口。

Tritium(config-vlan)# port *1/3 untagged*

Tritium(config-vlan)# port *1/8*

！ 设置 PVID

Tritium(config)# interface gigabitethernet *1/3*

Tritium(config-if)# switchport pvid *11*

！ 创建 VLAN 14。

Tritium(config)# vlan *14*

！ 向 VLAN 14 添加端口。

Tritium(config-vlan)# port *1/4 untagged*

Tritium(config-vlan)# port *1/8*

！ 设置 PVID

Tritium(config)# interface gigabitethernet *1/3*

Tritium(config-if)# switchport pvid *11*

Tritium(config)# interface gigabitethernet *1/4*

Tritium(config-if)# switchport pvid *14*

（3） 配置 switch3

！ 创建 VLAN 11。

Tritium(config)# vlan *11*

！ 向 VLAN 11 添加端口。

Tritium(config-vlan)# port *1/7,8*

！ 配置 VLAN 11 ip。

Tritium(config)# interface vlan *11*

Tritium(config-vlan-if)# ip address *172.168.11.84 255.255.255.0*

！ 创建 VLAN 14。

Tritium(config)# vlan *14*

！ 向 VLAN 14 添加端口。

Tritium(config-vlan)# port *1/8*

！配置 VLAN 14 ip。

Tritium(config)# interface vlan *14*

Tritium(config-vlan-if)# ip address *172.168.14.84 255.255.255.0*

（4） 配置 PC

！PC1 ip 172.168.11.11/24,网关 172.168.11.84

！PC2 ip 172.168.11.12/24,网关 172.168.11.84

！PC3 ip 172.168.11.13/24,网关 172.168.11.84

！PC4 ip 172.168.14.14/24,网关 172.168.14.84

4.2. VLAN 间路由

4.2.1. VLAN 间路由简介

Tritium S 系列交换机可在 VLAN 间实现路由功能。VLAN 间需要互相通信，需要在 VLAN 间配置路由，就像在 LAN 间配置网桥和交换机一样。配置 VLAN 间路由，必须要配置 VLAN 的三层接口和 VLAN 三层接口的 IP 地址。

4.2.2. VLAN 间路由配置

4.2.2.1. 进入 VLAN 接口配置模式

该命令用于进入 VLAN 接口配置模式，该 VLAN 必须是已经建立的。

表 4–3 进入 VLAN 接口配置模式

命令	命令模式	功能说明
interface vlan { *vlan-id* | *vlan-name* }	全局配置模式	进入某个 VLAN 接口配置模式。

参数说明：

vlan-id：该 VLAN 的 ID（1~4094）。

vlan-name：该 VLAN 的名字（字符串长度为 1~14）。

【示例】进入 VLAN 100 的 vlan 接口配置模式。

Tritium(config)# interface vlan *100*

Tritium(config-vlan-if)#

4.2.2.2. 配置 VLAN 接口的 IP 地址

配置 VLAN 接口 IP 地址的命令中，带 **secondary** 参数时配置的是从 IP 地址，可配置多个从地址，但必须先配置主 IP 地址。删除时，则需先删除从 IP 地址，或者不带地址参数删除所有 IP 地址。

表 4–4 进入 VLAN 接口配置模式

命令	命令模式	功能说明
ip address *IPAddr netmask* [**secondary**]	接口配置模式	配置 VLAN 接口的 IP 地址和子网掩码。
no ip address [*IPAddr netmask* [**secondary**]]	接口配置模式	删除 VLAN 接口 IP 地址配置。

4.2.3.VLAN 间路由配置实例

4.2.3.1. 组网需求

VLAN 3 和 VLAN 4 之间需要路由通信，其中 GE1/1 和 GE1/2 属于 VLAN 3，GE1/3 和 GE1/4 属于 VLAN 4。

4.2.3.2. 组网图

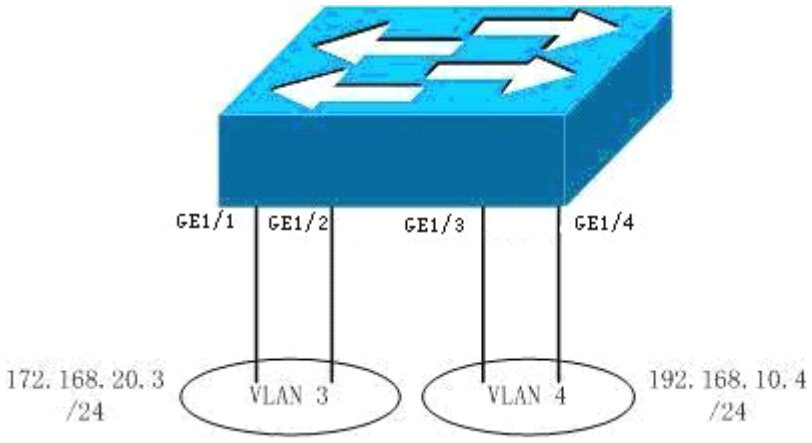


图 4–6 VLAN 间路由组网图

4.2.3.3. 配置步骤

！创建 VLAN 3

Tritium(config)# vlan *3* **name** *vlan3*

！添加端口

Tritium(config-vlan)# port *1/1,2* **untagged**

Tritium(config-vlan)# exit

！配置端口 PVID

Tritium(config)# interface gigabitethernet *1/1*

Tritium(config-if)# switchport pvid *3*

Tritium(config-if)# exit

Tritium(config)# interface gigabitethernet *1/2*

Tritium(config-if)# switchport pvid *3*

Tritium(config-if)# exit

！配置 VLAN 3 的 VLAN 接口

Tritium(config)# interface vlan *3*

Tritium(config-vlan-if)# ip address *172.168.20.3 255.255.255.0*

Tritium(config-vlan-if)# exit

！创建 VLAN 4

Tritium(config)# vlan *4* **name** *vlan4*

！添加端口

Tritium(config-vlan)# port *1/3,4* **untagged**

Tritium(config-vlan)# exit

！配置端口 PVID

Tritium(config)# interface gigabitethernet *1/3*

Tritium(config-if)# switchport pvid *4*

Tritium(config-if) exit

Tritium(config)# interface gigabitethernet *1/4*

Tritium(config-if)# switchport pvid *4*

Tritium(config-if)# exit

！配置 VLAN 4 的 VLAN 接口

Tritium(config)# interface vlan *4*

Tritium(config-vlan-if)# ip address *192.168.10.4 255.255.255.0*

4.3. Super VLAN

4.3.1. Super VLAN 概述

4.3.1.1. Super VLAN 背景

Super VLAN 又称为 VLAN 聚合（VLAN Aggregation），其原理是一个 Super VLAN 包含多个 Sub VLAN，Super VLAN 可配置虚接口的 IP 地址。每个 Sub VLAN 是一个广播域，不同 Sub VLAN 之间二层相互隔离，Sub VLAN 不能配置虚接口 IP 地址。当 Sub VLAN 内的用户需要进行三层通信时，将使用 Super VLAN 的虚接口的 IP 地址作为网关地址，这样多个 VLAN 共享一个 IP 地址，从而节省了 IP 地址资源。

为了实现不同 Sub VLAN 间的三层互通及 Sub VLAN 与其他网络的互通，需要利用 ARP 代理功能。通过 ARP 代理可以进行 ARP 请求和响应报文的转发与处理，从而实现了二层隔离端口间的三层互通。缺省状态下，Sub VLAN 下的 ARP 代理功能是关闭的。

4.3.1.2. Super VLAN 通信

下面描述一下 VLAN 聚合情况下，两个聚合的 Sub-VLAN 之间通信的过程，如下图所示：

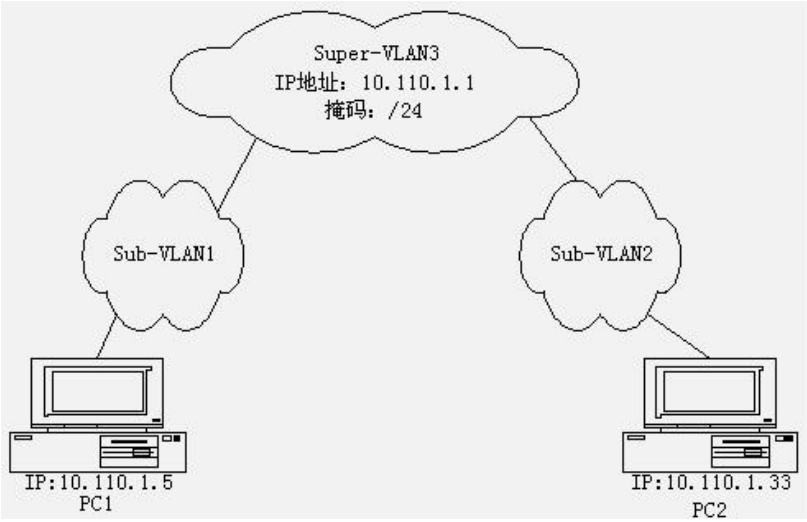


图 4-7 VLAN 聚合

Sub-VLAN 1 和 Sub-VLAN 2 聚合成 Super-VLAN 3，为 Super-VLAN 3 分配一个 IP 子网，则 Sub-VLAN 1 和 Sub-VLAN 2 都位于此子网。此处所指的 ARP 表是指 RPS 中的所有 ARP 表项。

若 Sub-VLAN 1 中的一台主机 PC 1 要与子网中的另一台主机 PC 2 通信，PC 1 发现对方

与自己处于同一网段，则直接发出目的 IP 为 10.110.1.33 的 ARP 请求报文。三层交换机收到后，由微码将其在 Sub-VLAN 1 的范围内直接通过二层广播此报文，并抄送一份给接口板的 ARP 模块。经过接口板 ARP 的分析，发现它来自 Sub-VLAN，就将此 ARP 请求报文交给主控板 ARP 模块处理。

主控板 ARP 首先在 ARP 表中查找 ARP 请求报文中的目的 IP 地址，如果找到对应项，看看目的 IP 地址是不是在 Sub-VLAN 1 中，是就丢弃该报文，不是就将 Super-VLAN 3 的 MAC 地址应答给 PC 1，完成代理工作。

如果在 ARP 表中没有找到对应项，主控板 ARP 就查 VLAN 聚合与 VLAN 的逻辑映射表，知道 Sub-VLAN 1 属于 Super-VLAN 3，将此报文中的源 MAC 地址替换成 Super-VLAN 3 的 MAC 地址，VLAN ID 的值由 1 分别替换成属于 Super-VLAN 3 的其它 Sub-VLAN 的值，之后逐个向属于此 Super-VLAN 的其它 Sub-VLAN（本例中为 Sub-VLAN 2）广播，并同时将此请求报文中的信息学习加入动态 ARP 表中。

此后若收到 PC 2 的 ARP 应答报文（其目的 MAC 地址为 Super-VLAN 3 的 MAC 地址），主控板 ARP 模块发现此 ARP 应答报文的 VLAN ID 是 Sub-VLAN 2，即 PC 2 位于 Sub-VLAN 2 中，主控板 CPU 根据应答报文中的信息，搜索 ARP 表中的各项，找到对应项后把 Super-VLAN 3 对应的 MAC 地址通过 ARP 应答报文回给 PC 1（若 PC 2 位于 Sub-VLAN 1，PC 2 响应的 ARP 应答报文直接通过二层转发回给 PC 1，交换机就不再应答）。同时在接口板上将 Sub-VLAN 2 中的响应报文信息记录在 ARP 表及 FIB 表中，以后再收到来自主机 X 的报文就可以通过查询 FIB 表进行三层转发了。

ARP Proxy 放在主控板上，这样可以避免由于不同接口板在同步上造成的差异，如我们从板 A 发出 ARP，从板 B 收到响应，但由于数据表格还没有同步到位板 B，则引起错误。

4.3.2.Super VLAN 配置

4.3.2.1. 创建 Super VLAN

Super VLAN 和普通 VLAN 共享 VLAN ID 号，因此要避免 Super VLAN 的 ID 和普通 VLAN ID 重复，否则将无法建立。

缺省情况下，没有任何 Super VLAN。

表 4–5 创建 Super VLAN

命令	命令模式	功能说明
supervlan *supervlan-id*	全局配置模式	创建一个 Super VLAN，并进入 supervlan 配置模式。
no supervlan *supervlan-id*	全局配置模式	删除某个 Super VLAN。

4.3.2.2. 配置 Super VLAN 成员

配置 Super VLAN 中的 VLAN 成员。

表 4–6 配置 Super VLAN 成员

命令	命令模式	功能说明
subvlan *vlan-list*	supervlan 配置模式	添加一个 VLAN 或 VLAN 列表到 Super VLAN 中。
no subvlan *vlan-list*	supervlan 配置模式	从 Super VLAN 中删除一个 VLAN 或 VLAN 列表。

4.3.2.3. 进入 Super VLAN 接口

表 4–7 进入 Super VLAN 接口

命令	命令模式	功能说明
interface supervlan *supervlan-id*	全局配置模式	进入 Super VLAN 的接口配置模式。

4.3.2.4. 配置 Super VLAN 代理

缺省情况下，是禁止 Super VLAN 的 ARP 代理。

表 4–8 配置 Super VLAN 代理

命令	命令模式	功能说明
supervlan proxy-arp	supervlan 接口配置模式	允许 Super VLAN 的 ARP 代理。
no supervlan proxy-arp	supervlan 接口配置模式	禁止 Super VLAN 的 ARP 代理。

4.3.2.5. 查看 Super VLAN 信息

表 4–9 查看 Super VLAN 信息

命令	命令模式	功能说明
show supervlan { *supervlan-id* | **all** }	特权用户模式	打印 Super VLAN 的相关信息。

4.3.3.Super VLAN 示例

4.3.3.1. 组网需求

创建一个 Super VLAN，加入三个 Sub VLAN，Sub VLAN 之间二层隔离，但可以三层通信。

4.3.3.2. 组网图

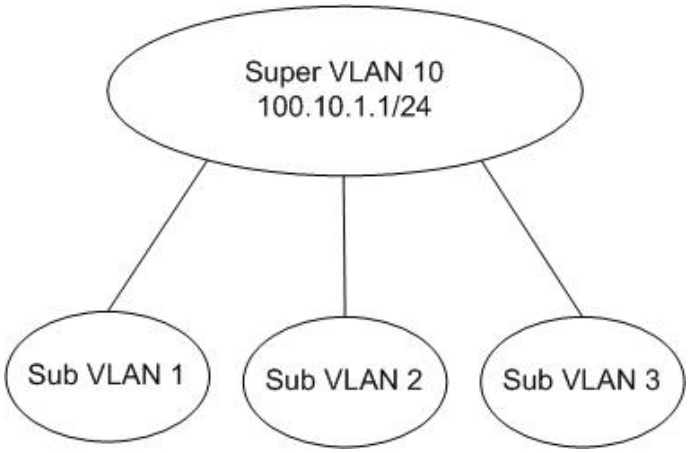


图 4–8 Super VLAN

4.3.3.3. 组网配置

！创建 Super VLAN 10

Tritium(config)# supervlan *10*

！配置 Super VLAN 10 成员 subvlan 1、2、3

Tritium(config-supervlan)# subvlan *1-3*

Tritium(config-supervlan)# exit

！配置 Super VLAN 10 的 IP 地址和 ARP 代理

Tritium(config)# interface supervlan *10*

Tritium(config-supervlan-if)# ip address *100.10.1.1 255.255.255.0*

Tritium(config-supervlan-if)# supervlan proxy-arp

第 5 章 生成树协议

5.1. 多生成树协议（MSTP）

多生成树（MST）把 IEEE802.1w 快速生成树(RST)算法扩展到多生成树，为虚拟局域网（VLANs）环境提供了快速收敛和负载均衡的功能；MST 比 PVST+收敛快并且和 802.1D、802.1w 生成树结构兼容。

5.1.1. 概述

MSTP（Multiple Spanning Tree Protocol）多生成树协议，用来在桥接局域网中建立简单而完整的拓扑结构。MSTP 可以与早期的 STP（Spanning Tree Protocol）和 RSTP（Rapid Spanning Tree Protocol）相兼容。

STP 和 RSTP 都只能在网络中建立单独的生成树拓扑，所有 VLAN 的报文沿着唯一的生成树进行转发。STP 收敛过慢，RSTP 通过握手机制保证网络拓扑快速稳定。

MSTP 继承了 RSTP 的快速握手机制，同时，在保证网络拓扑快速建立的基础上，MSTP 允许将不同的 VLAN 划分到不同的生成树中去，从而在网络中建立多个树状拓扑。在 MSTP 建立的网络中，属于不同 VLAN 的帧可以在不同的路径上转发，实现了 VLAN 数据的负载均衡。

与按 VLAN 划分 STP（per-VLAN Spanning Tree，PVST）不同的是，MSTP 还允许将多个 VLAN 划分到同一个生成树拓扑中去，这样可以有效减少支持大量 VLAN 所需的生成树的数目。

5.1.2. 多生成树区域

MSTP 中，VLAN 与生成树的对应关系是通过一个多生成树配置表来描述的。多生成树配置表，连同一个配置名称和一个配置修订号，共同构成了多生成树配置标识（MST Configuration Identifier）。

在网络上，相互连接且具有相同多生成树配置标识的网桥被认为是在同一个多生成树区

域（MST Region）中。同一个多生成树区域中的网桥通常也具有相同的 VLAN 配置，从而保证这些 VLAN 的帧只在区域内部流动。

5.1.3.IST, CST, CIST 和 MSTI

5.1.3.1. CIST

Common and Internal Spanning Tree，公共与内部生成树。是指网络中所有单个交换机及其连接的局域网构成的生成树。这些交换机可能分属不同的多生成树区域，也可能是运行传统 STP 或者 RSTP 协议的交换机，运行这两种协议的交换机在多生成树网络中被认为是处在仅由其自身组成的区域中。

网络拓扑稳定后，整个 CIST 会选出一个 CIST 根桥。每个区域内部也会选出 CIST 区域内根桥，作为从区域内部到达 CIST 根的最短路径。

5.1.3.2. CST

Common Spanning Tree，公共生成树。如果把每个多生成树区域看作是一个单独的交换机，CST 就是连接着所有这些“单独交换机”的生成树。

5.1.3.3. IST

Internal Spanning Tree，内部生成树。是指 CIST 在某个多生成树区域以内的部分。也可以理解为 IST 与 CST 共同构成了 CIST。

5.1.3.4. MSTI

Multiple Spanning Tree Instance，多生成树实例。MSTP 协议允许将不同的 VLAN 划分到不同的生成树中，从而就建立起多个生成树实例。通常情况下，编号为 0 的生成树实例是指 CIST，它可以扩展到整个网络，而从 1 开始所指的生成树实例，都处在某个区域的内部。每个生成树实例中都可以被分配多个 VLAN，初始情况下，所有的 VLAN 都被分配在 CIST 中。

多生成树区域中所有的 MSTI 都是相互独立的，它们可以选出不同的交换机作为各自的根。比如图 2.1 的区域 3 中，MSTI01 的根桥可能是处在左下角的交换机，而 MSTI00，也就

是 CIST 的区域内根桥则可能是处在中间位置的交换机。

5.1.4.稳定状态

MSTP 交换机根据接收到的 BPDU 执行计算和比较操作，最终可以使网络达到如下的稳定状态：

一台交换机被选为整个网络的 CIST 根（CIST Root）；

每个交换机和局域网段都会决定出到 CIST 根的具有最小开销的路径，以保证连接的完整性并防止环路；

每个区域内部都会选出一台交换机作为 CIST 区域内根（CIST Regional Root），该交换机具有到达 CIST 根的开销最小的路径；

每个 MSTI 都会独立的选择出一台交换机作为 MSTI 区域内根；

区域内部的每台交换机和局域网段都会确定出到达所在 MSTI 的根的开销最小的路径；

CIST 根端口（Root Port）提供经过 CIST 区域内根（如果该交换机不是 CIST 区域内根）到达 CIST 根（如果该交换机不是 CIST 根）的具有最小开销的路径；

CIST 指定端口（Designated Port）为所连接的局域网提供到达 CIST 根的最小开销路径；

Alternate 和 Backup 端口在交换机、端口或局域网失效或被移除时提供连接；

MSTI 根端口（Root Port）提供到达 MSTI 区域内根的最小开销路径（如果该交换机不是 MSTI 区域内根桥）；

MSTI 指定端口（Designated Port）为所连接局域网提供到达 MSTI 区域内根的最小开销路径；

一个主端口（Master Port）提供区域与区域外 CIST 根桥的连接。在区域内部，CIST 区域内根桥的 CIST 根端口会作为区域内所有 MSTI 的 Master 端口。

5.1.5.跳数

在区域内,与 STP 和 RSTP 不同，MSTP 协议不使用 BPDU 配置消息中的消息生存期（Message Age）和最大生存期（Max Age）来计算网络拓扑，而是使用了跳数属性（Hop

Count）。

为了防止旧的信息在网络中无休止的循环而影响新信息的传输，MSTP 使传输的信息在每个生成树中都与一个跳数属性相关联。BPDU 的跳数属性由 CIST 区域内根桥或者 MSTI 区域内根桥指定，并在每个接收端口处被减小。如果跳数在端口处变为了 0，该信息会被丢弃同时该端口会成为一个指定端口。

5.1.6.STP 兼容性

MSTP 协议允许交换机通过一种协议转换机制与传统的 STP 交换机协同工作。如果交换机的一个端口接收到 STP 的配置信息，那么该端口就会转为仅发送 STP 报文。同时，接受到 STP 信息的端口也会被认为是一个边界端口。

注意：

一个端口转入 STP 兼容状态之后，即使不再接收到 STP 报文，该端口也不会自动恢复为 MSTP 状态。这种情况下，可以使用 mstp mcheck 命令清除端口学习到的生成树协议信息，使之恢复为 MSTP 状态。

运行 RSTP 协议的交换机可以识别并处理 MSTP 报文，因此与 RSTP 交换机协同工作时 MSTP 交换机不需要发生协议转换。

5.1.7.BPDU 的格式

BPDU 消息的格式如下表：

DMA	SMA	L/T	LLC Header	Payload

- DMA：目的 MAC 地址——BPDU 的目的地址是一个固定的交换机的组播地址（0x0180c2000000）
- SMA：源 MAC 地址——即发送该配置消息的交换机 MAC 地址
- L/T：帧长
- LLC Header：BPDU 固定的链路头
- Payload：BPDU 数据

下表为 Payload 中的 BPDU 数据内容：

值域	字节位	占有字节
Protocol Identifier	1~2	2
Protocol Version Identifier	3	1
BPDU Type	4	1
CIST Flags	5	1
CIST Root Identifier	6~13	8
CIST External Path Cost	14~17	4
CIST Regional Root Identifier	18~25	8
CIST Port Identifier	26~27	2
Message Age	28~29	2
Max Age	30~31	2
Hello Time	32~33	2
Forward Delay	34~35	2
Version 1 Length = 0	36	1
Version 3 Length	37~38	2
MST Configuration Identifier	39~89	51
CIST Internal Root Path Cost	90~93	4
CIST Bridge Identifer	94~101	8
CIST Remaining Hops	102	1
MSTI Configuration Messages (may be absent)	103-39+Version 3 Length	

MSTI Configuration Message 的内容如下：

值域	字节位	占有字节
MSTI Flags	1	1
MSTI Regional Root Identifier	2~9	8
MSTI Internal Root Path Cost	10~13	4
MSTI Bridge Priority	14	1
MSTI Port Priority	15	1
MSTI Remaining Hops	16	1

5.2. 生成树协议的配置任务

MSTP 允许在启动它之前配置设备或以太网接口端口的相关参数，在各项配置任务中，只有启动 MSTP 后，它们才能生效。

5.2.1.MSTP 配置

5.2.1.1. 开启设备或接口上的 MSTP 协议

该命令用来开启设备或接口上的 MSTP 协议。

表 5–1 开启设备或接口上的 MSTP 协议

命令	命令模式	功能说明
mstp { **enable** | **disable** }	全局配置模式 以太网接口配置模式 potr-trunk 接口配置模式	开启/关闭设备或接口上的 MSTP 协议。

参数说明：

enable：用来开启设备或接口的 MSTP 协议。

disable：用来关闭设备或接口的 MSTP 协议。

缺省情况下，以太网交换机禁用 MSTP。设备 MSTP 启动时，在所有接口上缺省为开启 MSTP 协议。

如果在启动设备 MSTP 协议前，没有配置设备或接口的其它 MSTP 协议参数，则这些参数均为缺省值。MSTP 协议启动后，可以采用配置命令来配置设备或接口的 MSTP 协议参数。在全局配置模式下执行此命令是开启设备的 MSTP 协议；在以太网接口配置模式下执行此命令是开启接口的 MSTP 协议。

【示例】开启设备的 MSTP 协议。

```
Tritium(config)# mstp enable
```

5.2.1.2. 设置接口的路径开销

该命令用来设置指定实例当前以太网接口的路径开销，此命令的 **no** 形式用来恢复指定实例当前以太网接口的路径开销为缺省值。

表 5–2 设定接口的路径开销

命令	命令模式	功能说明
mstp *instance-id* **cost** *cost*	以太网接口配置模式 port-trunk 接口配置模式	设置当前以太网接口在指定实例中的路径开销。
no mstp *instance-id* **cost**	以太网接口配置模式 port-trunk 接口配置模式	恢复当前以太网接口在指定实例中的路径开销为缺省值。

参数说明：

instance-id：用来标识实例 ID，范围 0~15。

cost：用来标识所设定的路径开销值，范围 1~200 000 000。

缺省情况下，网桥由与接口相连的链路速率而直接得到接口的路径开销。

接口的路径开销和与该接口相连的链路速率有关，见下表所示。MSTP 协议可以通过查询与该接口相连的链路速率而直接得到接口的路径开销。建议用户使用缺省值，由 MSTP 协议来查询接口的路径开销值。

链路速率	推荐值	推荐取值范围	值域
10Mbit/s	2 000 000	200 000~20 000 000	1~200 000 000
100Mbit/s	200 000	20 000~2 000 000	1~200 000 000
1Gbit/s	20 000	2 000~200 000	1~200 000 000
10Gbit/s	2 000	200~20 000	1~200 000 000

【示例】设置当前接口在实例 0 中的路径开销为 1000。

Tritium(config-if)# mstp *0* **cost** *1000*

5.2.1.3. 配置置交换机接口为（非）边缘端口

该命令用来配置交换机接口为边端接口，此命令的 **no** 形式用来设置交换机的接口为非边缘端口。缺省情况下，端口为边缘端口。

表 5–3 配置置交换机接口为（非）边缘端口

命令	命令模式	功能说明
mstp edge	以太网接口配置模式 port-trunk 接口配置模式	配置交换机接口为边缘端口。
no mstp edge	以太网接口配置模式 port-trunk 接口配置模式	设置交换机接口为非边缘端口。

【示例】设置该接口为边缘端口。

Tritium(config-if)# mstp edge

5.2.1.4. 设置交换机的 Forward Delay 时间参数

该命令用来设置交换机的 Forward Delay 时间参数，此命令的 **no** 形式用来恢复该时间

参数为缺省值。缺省值为 15 秒。

表 5–4 设置交换机的 Forward Delay 时间参数

命令	命令模式	功能说明
mstp forward-time *seconds*	全局配置模式	设置交换机的 Forward Delay 时间参数。
no mstp forward-time	全局配置模式	恢复该时间参数为缺省值。

参数说明：

seconds：用来标识所设置的 Forward Delay 时间参数值，单位为秒，范围 4~30。

设备的 Forward Delay 时间参数值与交换网络的网络直径有关，网络直径越大，Forward Delay 时间值就越大，可以通过该命令来改变设备的 Forward Delay 时间参数值。建议使用缺省值 15 秒。

【示例】设置交换机的 Forward Delay 时间参数为 18 秒。

Tritium(config)# mstp forward-time *18*

5.2.1.5. 设置交换机的 Max Age 时间参数

该命令用来设置交换机的 Max Age 时间参数，此命令的 **no** 形式用来恢复该时间参数为缺省值。缺省值为 20 秒。

表 5–5 设置交换机的 Max Age 时间参数

命令	命令模式	功能说明
mstp max-age *seconds*	全局配置模式	设置交换机的 Max Age 时间参数。
no mstp max-age	全局配置模式	恢复该时间参数为缺省值。

参数说明：

seconds：用来标识所设置的 Max Age 时间参数值，单位为秒，范围 6~40。

Max Age 时间是用来判断 MSTP 协议报文是否“过时”的参数，如果这个值太小，生成树计算就会比较频繁，有可能将网络拥塞误认为是链路故障；如果这个值太大，则不利于及时发现链路故障。Max Age 时间值与交换网络的网络直径有关，用户根据实际情况可以使用该命令来改变 Max Age 时间参数值。建议使用缺省值 20 秒。

【示例】设置交换机的 Max Age 时间参数 18 秒。

Tritium(config)# mstp max-age *18*

5.2.1.6. 设置交换机的 Hello Time 时间参数

该命令用来设置交换机的 Hello Time 时间参数，此命令的 **no** 形式用来恢复该时间参数为缺省值。缺省值为 2 秒。

表 5–6 设置交换机的 Hello Time 时间参数

命令	命令模式	功能说明
mstp hello-time *seconds*	全局配置模式	设置交换机的 Hello Time 时间参数。
no mstp hello-time	全局配置模式	恢复该时间参数为缺省值。

参数说明：

seconds：用来标识所设置的 Hello Time 时间参数值，单位为秒，范围 1~10。

交换机作为网络根桥时，Hello Time 时间是用于控制指定端口发送配置信息的时间间隔，如果这个值太小，报文发送过于频繁，有可能导致网络带宽占用率过大；如果这个值过大，则不能及时发现拓扑变化。用户根据实际情况可以使用该命令来改变 Hello Time 时间参数值。建议使用缺省值 2 秒。

【示例】设置交换机的 Hello Time 时间参数 5 秒。

Tritium(config)# mstp hello-time *5*

5.2.1.7. 设置 MSTP 协议的工作模式

如果在与当前以太网接口相连的网段内存在运行 STP 协议的网桥，该接口会迁移到 STP 兼容模式下运行。在网络比较稳定的情况下，虽然网段内运行 STP 协议的网桥被拆离，但与之相连的运行 MSTP 协议的交换机的接口仍然会运行在 STP 兼容模式下，此时可以通过该命令迫使其迁移到 MSTP 模式下运行。接口迁移到 MSTP 模式下运行后，如果再次收到新的 STP 报文，接口又会回到 STP 兼容模式下。

表 5–7 设置 MSTP 协议的工作模式

命令	命令模式	功能说明
mstp mcheck	以太网接口配置模式 port-trunk 接口配置模式	设置为 MSTP 协议的工作模式。

【示例】将运行 MSTP 协议的接口从 STP 兼容模式下迁移到 MSTP 模式下运行。

Tritium(config-if)# mstp mcheck

5.2.1.8. 设置与接口相连的链路是否是点到点链路

该命令用来设置与当前以太网接口相连的链路是否是点到点链路，此命令的 **no** 形式用来恢复为缺省状态，即由 MSTP 协议来检测与该以太网接口相连的链路是否是点到点链路。

表 5–8 设置与接口相连的链路是否是点到点链路

命令	命令模式	功能说明
mstp point-to-point { **forcetrue** | **forcefalse** | **auto** }	以太网接口配置模式 port-trunk 接口配置模式	设置与当前以太网接口相连的链路是否是点到点链路。
no mstp point-to-point	以太网接口配置模式 port-trunk 接口配置模式	恢复为缺省状态。

参数说明：

forcetrue：用来标识与当前以太网接口相连的链路是点到点链路。

forcefalse：用来标识与当前以太网接口相连的链路不是点到点链路。

auto：采用自动方式检测与该以太网接口相连的链路是否是点到点链路。

缺省为 **auto**。如果当前以太网接口工作在全双工模式，则当前接口相连的链路就是点到点链路。建议用户使用缺省值，由 MSTP 协议来进行自动检测。

【示例】设置与当前以太网接口相连的链路是点到点链路。

```
Tritium(config-if)# mstp point-to-point forcetrue
```

5.2.1.9. 设置接口优先级

该命令用来设置当前以太网接口在指定实例中的优先级，此命令的 **no** 形式用来恢复当前以太网接口在指定实例中的优先级为缺省值。缺省优先级为 128。

表 5–9 设置接口优先级

命令	命令模式	功能说明
mstp *instance-id* **port-priority** *port-priority*	以太网接口配置模式 port-trunk 接口配置模式	设置当前以太网接口在指定实例中的优先级。
no mstp *instance-id* **port-priority**	以太网接口配置模式 port-trunk 接口配置模式	恢复当前以太网接口在指定实例中的优先级为缺省值。

参数说明：

instance-id：用来标识实例 ID，范围 0~15。

port-priority：用来标识所设置的优先级，该值是不连续的，取值 0~240，步长为 16。

可以采用该命令设置当前接口的优先级，优先级取值必须为 16 的倍数，如 0、16、32、48 等，数值越小，表示优先级越高，该接口就越有可能成为根接口。

【示例】设置接口在实例 0 中的优先级为 16。

Tritium(config-if)# mstp *0* **priority** *16*

5.2.1.10. 设置交换机的 bridge 优先级

该命令用来设置交换机在指定实例中的 bridge 优先级，此命令的 **no** 形式用来恢复交换机在指定实例中的 bridge 优先级为缺省值。缺省 bridge 优先级为 32768。

表 5–10 设置交换机的 bridge 优先级

命令	命令模式	功能说明
mstp *instance-id* **priority** *bridge-priority*	全局配置模式	设置交换机在指定实例中的 bridge 优先级。
no mstp *instance-id* **priority**	全局配置模式	恢复交换机在指定实例中的 bridge 优先级为缺省值。

参数说明：

instance-id：用来标识实例 ID，范围 0~15。

bridge-priority：用来标识所设置的 bridge 优先级，该值是不连续的，范围为 0~61440，步长为 4096。

可以采用该命令设置交换机在指定实例中的 bridge 优先级，优先级取值必须为 4096 的倍数，如 0、4096、8192 等，数值越小，表示优先级越高，该交换机就越有可能成为该交换网络的根桥。

【示例】设置交换机在实例 0 中的 bridge 优先级为 8192。

Tritium(config)# mstp *0* **priority** *8192*

5.2.1.11. 设置多生成树区域名称

该命令用来设置交换机在多生成树区域中的名称，此命令的 **no** 形式用来恢复交换机在多生成树区域中的名称为缺省值。缺省为本交换机的 MAC 地址。

表 5–11 设置多生成树区域名称

命令	命令模式	功能说明
mstp name *string*	全局配置模式	设置多生成树区域名称。
no mstp name	全局配置模式	恢复多生成树区域名称为缺省值。

参数说明：

string：配置多生成树区域名称，最多可包含 32 个字符，大小写敏感。

【示例】设置多生成树区域名称为 galaxywind。

Tritium(config)# mstp name *galaxywind*

5.2.1.12. 设置多生成树区域修订号

该命令用来设置交换机在多生成树区域中的修订号，此命令的 **no** 形式用来恢复交换机在多生成树区域中的修订号为缺省值。缺省为 0。

表 5–12 设置多生成树区域修订号

命令	命令模式	功能说明
mstp revision *value*	全局配置模式	设置多生成树区域修订号。
no mstp revision	全局配置模式	恢复多生成树区域修订号为缺省值。

参数说明：

value：配置多生成树区域修订号，范围 0~65535。

【示例】设置多生成树区域修订号为 1024。

Tritium(config)# mstp revision *1024*

5.2.1.13. 设置多生成树实例

该命令用来设置生成树实例，并将指定 VLAN 添加到实例中，此命令的 **no** 形式用来删除实例或者将从指定 VLAN 中将实例中删除。

表 5–13 设置多生成树实例

命令	命令模式	功能说明
mstp instance *instance-id* [**vlan** *vlan-list*]	全局配置模式	设置多生成树实例。

no mstp instance *instance-id* [**vlan** *vlan-list*]	全局配置模式	删除多生成树实例或者将指定VLAN从实例中删除

参数说明：

instance-id：用来标识实例ID，范围1~15。CIST实例中不允许配置/删除VLAN.

vlan-list：VLAN ID，范围1~4094。

【示例】配置多生成树实例2，并将VLAN ID为2，3，6的VLAN加入MSTID2。

Tritium(config)# mstp instance *2* **vlan** *2-3,6*

5.2.1.14. 设置多生成树网络直径

网络直径表示网络上两台主机之间跨越交换机的最大数目，它反映了网络的规模。可以通过下列命令设置多生成树协议的网络直径。

表 5–14 设置多生成树网络直径

命令	命令模式	功能说明
mstp diameter *net-diameter*	全局配置模式	设置网络直径参数
no mstp diameter	全局配置模式	恢复网络直径参数为默认值

参数说明：

net-diameter：网络直径。范围2~7，默认值为7。

网络直径参数仅对CIST有效，且在交换机中并没有作为一项单独的设置而被保存，设置网络直径参数后，生成树协议的三个时间参数会被自动更新为较优的值。

【示例】配置多生成树网络直径为6。

Tritium(config)# mstp diameter 6

5.2.1.15. 设置多生成树最大跳数

可以通过下列命令设置多生成树协议的最大跳数。

表 5–15 设置多生成树最大跳数

命令	命令模式	功能说明
mstp max-hops *hop-count*	全局配置模式	设置最大跳数

no mstp max-hops	全局配置模式	恢复最大跳数参数为默认值

参数说明：

hop-count：最大跳数。范围 1~40，默认值为 20。

【示例】配置多生成树最大跳数为 26。

Tritium(config)# mstp max-hops 26

5.2.1.16. 设置接口优先级

在连接 Cisco 6509 设备的接口下使能该命令，防止该接口受到 mstp 报文时，因为摘要不匹配而将其作为 RSTP 报文处理。

表 5–16 设置接口优先级

命令	命令模式	功能说明
mstp digest-snooping	以太网接口配置模式	接口使能兼容摘要计算
no mstp digest-snooping	以太网接口配置模式	接口删除兼容摘要计算

5.2.1.17. 监控和维护 MSTP

在完成上述配置后，执行 **show** 命令可以查看 MSTP 的运行信息。根据该命令的输出信息，可以帮助用户确认 MSTP 配置是否正确，然后进行 MSTP 故障的排除。

表 5–17 监控和维护 MSTP

命令	命令模式	功能说明
debug switch mstp { **all** | **error** | **role** | **bpdu-rx**| **bpdu-tx** | **state**| **trace** }	特权用户模式	用来开启当前 MSTP 协议运行时供用户查看的 debug 信息，包含有错误信息、端口角色、接收报文、发送报文、状态迁移 6 个参数。
no debug switch mstp { **all** | **role** | **bpdu-rx**| **bpdu-tx** | **state**| **trace** }	特权用户模式	关闭用户 debug 信息开关。
show mstp [**instance** *instance-id*]	特权用户模式	显示多生成树协议信息，不带 instance 子命令时显示所有生成树实例信息
show mstp region	特权用户模式	显示多生成树协议的区域配置信息。
show mstp detail	特权用户模式	显示多生成树协议的详细信息。
show mstp interfaces {*interface-type interface-num*}	特权用户模式	显示当前接口下 MSTP 协议的状态信息或统计信息

参数说明：

interface-type：接口类型（fastethernet、gigabitethernet、10gigabitethernet、port-trunk）。

interface-num：接口号，格式为 *slot/port*。

instance-id：实例 ID，范围为 0~15。

trace：Mstp trace information debuging。

【示例】显示 Gigabitethernet 4/2 接口的 MSTP 协议的信息。

Tritium# show mstp interface gigabitethernet *4/2*

Giga 4/2 of MST0 is Designated Forwarding

Port Info Port ID: 80.402 Pri:128 Cost: 20000

Designated Root Address: 000fe284db30 Pri:32768 ExtCost: 200000

CIST Regional Root Address: 0011f7012453 Pri:32768 IntCost: 0

Designated Bridge Address: 0011f7012453 Pri:32768 Port ID: 80.402

Point-to-point admin: Auto oper: Yes

Edge admin: Y oper: Y

Bpdu Guard: False Root Guard: False

Loop Guard: False

Bpdu Skewing: False

Bpdu Filtering: False

TC Guard: False

MSTP Err-disable time: 300

MST BPDU tx: 7738

RSTP BPDU rx: 0

CONFIG BPDU rx: 0

TCN BPDU rx: 0

Instance Role Sts Cost Pri.Nbr Vlans Mapped

--------- ---- --- ---- -------------- -------------

0 D Fwd 20000 80.402 1-4094

5.3. MSTP 配置实例

5.3.1.组网需求

配置区域名称为 galaxywind，修订号为 1024。区域内配置一个多生成树实例，且实例 ID 为 1，并且将 VLAN 20 关联到实例中。

5.3.2.组网图

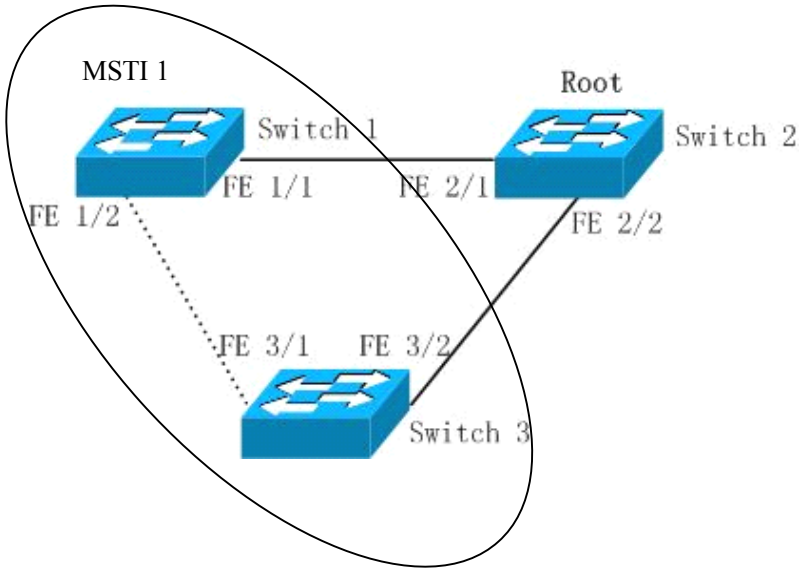


图 5–1 MSTP 组网图

5.3.3.组网配置

Switch 1 :

！创建 VLAN 20，将端口 FE1/1,FE1/2 加入 VLAN

Tritium(config)# vlan *20*

Tritium(config-vlan)#port 1/1,2

Tritium(config-vlan)#exit

！配置区域名称 galaxywind，修订号 1024

Tritium(config)# mstp name *galaxywind*

Tritium(config)# mstp revision *1024*

！配置实例 1，并将 VLAN20 关联到实例中

Tritium(config)# mstp instance-id *1* **vlan** *20*

Switch 3:

！创建 VLAN 20，将端口 FE3/1,FE3/2 加入 VLAN

Tritium(config)# vlan *20*

Tritium(config-vlan)#port 3/1,2

Tritium(config-vlan)#exit

！配置区域名称 galaxywind，修订号 1024

Tritium(config)# mstp name *galaxywind*

Tritium(config)# mstp revision *1024*

！配置实例 1，并将 VLAN20 关联到实例中

Tritium(config)# mstp instance-id *1* **vlan** *20*

Switch 2:

缺省配置。

第 6 章 MSTP 安全防护

6.1. MSTP 安全防护

6.1.1. Mstp Bpdu Guard 简介

对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接受到配置消息（BPDU 报文）时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑的震荡。这些端口正常情况下应该不会收到生成树协议的配置消息的。如果有人伪造配置消息恶意攻击交换机，就会引起网络震荡。BPDU 保护功能可以防止这种网络攻击。

交换机上启动了 BPDU 保护功能以后，如果端口收到了配置消息，系统就将这些端口设置为 BLK 状态，同时通知网管。接口配置 BPDU Guard 后，一旦接收到 BPDU，立刻进入 BLK 状态，根据设置了的 err-disable 值，在 err-disable 减至 0 后，恢复接口；

6.1.2. Mstp Loop Guard 简介

防止一个阻断的端口由于链路不正常（不能双向通信等）接不到 BPDU 后变成转发。如果 blocking 端口未收到 BPDU，则可能从 Alternate Port 或者 Backup Port 转换为 Designated Port，从而形成新的环路。Loop Guard 功能加入了其它检查，如果 non-designated Port 没有收到 BPDU，且 Loop Guard 功能已经使能的情况下，而该接口转到 loop-inconsistent blocking 状态，而不是 listening/learning/forwarding 状态。

6.1.3. Mstp Root Guard 简介

为了防止客户交换机偶然成为根桥，可以在连接到客户交换机的端口上使用 Root Guard 特性来避免这一问题的发生。如果 STP 偶然选出与客户交换机连接的某个端口做为根端口(RP)，那么 Root Guard 特性将把该端口设置为 root-inconsistent 状态(即 BLK 状态)来防止客户交换机成为根桥。Root Guard 功能对于设置了 Root Guard 功能的端口，端口角色只能保持为指定端口。一但接口上收到了更优的配置消息，则该端口进入 root-inconsistent 状态(即

BLK 状态)，不再转发报文(相当于将些端口相连的链路断开)。根据设置了的 err-disable 值，在 err-disable 减至 0 后，恢复接口。

6.1.4.Mstp Bpdu Filter 简介

通过使用 BPDU 过滤功能，将能够防止交换机在接口上发送 BPDU。对于边界端口，它通常连接到主机设备，因为主机不需要参与 STP，所有它将丢弃所接收到的 BPDU。通过使用 BPDU 过滤功能，将能够防止向主机设备发送不必要的 BPDU。在接口上明确配置了 BPDU 过滤功能，那么交换机将不发送任何的 BPDU，并且将把接收到的所有 BPDU 都丢弃。注意，如果在链接到其他交换机的端口上配置了 BPDU 过滤，那么就有可能导致桥接环路，所以在部署 BPDU 过滤时要格外小心，一般我们不推荐使用 BPDU 过滤。如果在与启用了 BPDU 过滤的相同接口上配置了 BPDU 保护，因为 BPDU 过滤的优先级高于 BPDU 保护，所以 BPDU 保护将不起作用。

6.1.5.Mstp Bpdu Skewing 简介

生成树（STP）的工作主要依赖于桥协议数据单元（BPDU）的定时接收，BPDU 是每隔 hello_time（缺省为 2 秒钟）的时间由根桥（root bridge）发送，也就是说每隔 hello_time 的时间，每个非根桥会从根桥接收到 BPDU。有时，BPDU 会丢失或桥的 CPU 太忙而延迟 BPDU 的定时转发，这会引起 BPDU 的延迟到达，从而潜在地影响生成树（STP）拓扑结构的稳定。BPDU skew（BPDU 迟滞）检测允许交换机跟踪迟到的 BPDU 并通过 syslog 信息通知管理员，对于每个收到了迟到 BPDU 的端口，迟滞检测会报告最近的迟滞和延迟的持续时间，它也报告有关这个端口的最长 BPDU 延迟。为了避免桥 CPU 的负载过大，syslog 信息不会在每次 BPDU 迟滞发生时产生，而是每隔 60 秒发一条信息；如果 BPDU 的延迟超过了 max_age/2（缺省是 10 秒），syslog 信息总是立即产生。BPDU 迟滞检测是一个诊断功能，它不会采取进一步的矫正功能。

6.1.6.Mstp Tc Guard 简介

通过使用 TC Guard 功能，可以防止 TC-BPDU 报文攻击。功能正常情况下，当交换机收到 TC-BPDU 报文后，会执行 MAC 地址表项和 ARP 表项的删除操作。因此当有人故意

伪造 TC-BPDU 报文恶意攻击交换机时，短时间内交换机会收到大量的 TC-BPDU 报文，造成交换机频繁的删除本机的 MAC 地址表，导致 ARP 地址表不停的刷新，影响 MSTP 的计算并占用大量的网络带宽，还造成交换机 CPU 占用率居高不下。开启防止 TC-BPDU 报文攻击功能后，交换机会在收到 TC-BPDU 报文后，进行一次删除 MAC 地址表和 ARP 表项的操作，并同时启动周期为 10 秒的定时器。在此周期时间内，如果交换机再次收到 TC-BPDU 报文，则交换机最多可以进行 6 次删除 MAC 地址表项和 ARP 表项的操作。从而避免频繁的删除 MAC 地址表和 ARP 表项，给交换机进行 MSTP 计算以及网络稳定性带来恶劣的影响。用户还可以配置一个周期内删除 MAC 地址表和 ARP 表项操作次数的上限值（通过命令 global mstp tc-protection threshold 设定）。如果在周期时间内，交换机收到 TC-BPDU 报文的次数少于上限值，则收到一个 TC-BPDU 报文进行一次删除操作；如果在周期时间内收到的 TC-BPDU 报文的次数，超过了用户设定的上限值，则交换机按照设定的上限值次数进行删除操作。举例来说，用户设定周期时间内，交换机进行 MAC 地址表和 ARP 表项删除操作的上限值为 100，实际一个周期内交换机收到 200 个 TC-BPDU 报文，则交换机只删除 MAC 地址表和 ARP 地址表 100 次。

6.1.7.MSTP 安全防护配置

6.1.7.1. 使能/禁止 mstp bpdu-guard

表 6–1 使能/禁止 mstp bpdu-guard

命令	命令模式	功能说明
mstp bpdu-guard enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 mstp bpdu-guard 功能。
mstp bpdu-guard disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 mstp bpdu-guard 功能。
global mstp bpdu-guard enable	全局配置模式	全局使能 mstp bpdu-guard 功能。
global mstp bpdu-guard disable	全局配置模式	全局禁止 mstp bpdu-guard 功能。

注意：该功能缺省禁用。

6.1.7.2. 使能/禁止 mstp loop-guard

表 6–2 使能/禁止 mstp loop-guard

命令	命令模式	功能说明
mstp loop-guard enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 mstp loop-guard 功能。
mstp loop-guard disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 mstp loop-guard 功能。

注意：该功能缺省禁用。

6.1.7.3. 使能/禁止 mstp root-guard

表 6–3 使能/禁止 mstp root-guard

命令	命令模式	功能说明
mstp root-guard enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 mstp root-guard 功能。
mstp root-guard disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 mstp root-guard 功能。

注意：该功能缺省禁用。

6.1.7.4. 使能/禁止 mstp tc-guard

表 6–4 使能/禁止 mstp tc-guard

命令	命令模式	功能说明
mstp tc-guard enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 tc-guard 功能。
mstp tc-guard disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 tc-guard 功能。
global mstp tc-guard enable	全局配置模式	全局使能 tc-guard 功能。
global mstp tc-guard disable	全局配置模式	全局禁止 tc-guard 功能。
global mstp tc-protection threshold <1-255>	全局配置模式	配置 10S 周期内允许更新 ARL 及 ARP 表的阀值，默认值为 6。
no global mstp tc-protection threshold	全局配置模式	恢复 10S 周期内允许更新 ARL 及 ARP 表的阀值为默认值。

注意：该功能缺省禁用。

6.1.7.5. 使能/禁止 mstp bpdu-filter

表 6–5 使能/禁止 mstp bpdu-filter

命令	命令模式	功能说明
mstp bpdu-filter enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 bpdu-filter 功能。
mstp bpdu-filter disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 bpdu-filter 功能。
global mstp bpdu-filter enable	全局配置模式	全局使能 bpdu-filter 功能。
global mstp bpdu-filter disable	全局配置模式	全局禁止 bpdu-filter 功能。

注意：该功能缺省禁用。

6.1.7.6. 使能/禁止 mstp bpdu-skewing

表 6–6 使能/禁止 mstp bpdu-skewing

命令	命令模式	功能说明
mstp bpdu-skewing enable	以太网接口配置模式 port-trunk 接口配置模式	接口使能 bpdu-skewing 功能。
mstp bpdu-skewing disable	以太网接口配置模式 port-trunk 接口配置模式	接口禁止 bpdu-skewing 功能。
global mstp bpdu-skewing enable	全局配置模式	全局使能 bpdu-skewing 功能。
global mstp bpdu-skewing disable	全局配置模式	全局禁止 bpdu-skewing 功能。

注意：该功能缺省禁用。

6.1.7.7. 配置 mstp err-disable time

表 6–7 配置 mstp err-disable time

命令	命令模式	功能说明
global mstp err-disable time <*30,65535*>	全局配置模式	配置 mstp err-disable time 值
no global mstp err-disable time	全局配置模式	恢复 mstp err-disable time 为默认值

mstp err-disable time 默认值为 300。

第7章 安全防护

7.1. DHCP snooping

7.1.1.dhcp snoop 简介

适用平台：

Bcm 所有交换机平台

DHCP 协议是在 UDP 和 IP 协议的基础上运行，有很多不安全因素。而且 DHCP 的运作机制中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，将会给网络照成混乱。交换机可以通过运行在数据链路层的 DHCP Snooping 功能来监听 DHCP 报文，记录服务器分配给客户端的 IP 地址等配置信息，并通过与交换机上其它功能模块的配合，提高整体网络的安全性。

DHCP Snooping 的信任端口功能所提供的是对于 DHCP 服务器信息来源的控制，此功能通过将不信任端口接收的 DHCP 响应报文丢弃，防止 DHCP 客户端从网络中不可信任的 DHCP 服务器获取 IP 地址。信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的DHCP 报文正常转发，从而保证了DHCP 客户端获取正确的IP 地址。不信任端口是不与合法的 DHCP 服务器连接的端口。如果从不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文则会丢弃，从而防止了 DHCP 客户端获得错误的 IP 地址。

7.1.2.dhcp snoop 配置

7.1.2.1. 使能 dhcp snoop

该命令用于开启或者关闭 dhcp snoop 功能。

表 7–1 使能/禁止 dhcp snoop

命令	命令模式	功能说明
ip dhcp snooping **no ip dhcp snooping**	全局配置模式或者 端口配置模式	开启 dhcp snooping 功能 No 命令为关闭 dhcp snooping 功能

【示例】将 1/1 的 dhcp snoop 功能开启

Tritium(config-if)# ip dhcp snooping

7.1.2.2. 设置 dhcp snoop 受信端口

该命令用于设置和取消 dhcp snoop 受信端口。

表 7–2 配置/取消 dhcp snoop 受信端口

命令	命令模式	功能说明
ip dhcp snooping trust **no ip dhcp snooping trust**	端口配置模式	设置 dhcp snooping 受信端口 No 命令为删除 dhcp snooping 受信端口

【示例】将端口 1/2 设置为 dhcp snooping 受信端口

Tritium(config-if)# ip dhcp snooping trust

7.1.2.3. 显示 dhcp snoop 配置信息

该命令用于显示 dhcp snoop 的配置信息。

表 7–3 显示 dhcp snoop 配置信息

命令	命令模式	功能说明
show dhcpsnooping database	特权用户模式	**显示 dhcp snoop 配置信息**

【示例】显示 dhcp snoop 的配置信息

Tritium# show dhcpsnooping database

7.2. DHCPv6 snooping

7.2.1. dhcpv6 snoop 简介

DHCPv6 协议是在 UDP 和 IP 协议的基础上运行，有很多不安全因素。而且 DHCPv6 的运作机制中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，将会给网络照成混乱。交换机可以通过运行在数据链路层的 ipv6 DHCP Snooping 功能来监听 DHCPv6 报文，记录服务器分配给客户端的 IP 地址等配置信息，并通过与交换机上其它功能模块的配合，提高整体网络的安全性。

DHCPv6 Snooping 的信任端口功能所提供的是对于 DHCP 服务器信息来源的控制，此功能通过将不信任端口接收的 DHCPv6 响应报文丢弃，防止 DHCP 客户端从网络中不可信任的 DHCP 服务器获取 IP 地址。信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的 DHCPv6 报文正常转发，从而保证了 DHCP 客户端获取正确的 IP 地址。不信任端口是不与合法的 DHCP 服务器连接的端口。

7.2.2. ipv6 dhcp snooping 配置

7.2.2.1. 使能 ipv6 dhcp snooping

该命令用于使能或禁止 ipv6 dhcp snooping 功能。

表 7–4 使能/禁止 dhcp snoop

命令	命令模式	功能说明
ipv6 dhcp snooping	全局配置模式 端口配置模式	开启 ipv6 dhcp snooping 功能
no ipv6 dhcp snooping	全局配置模式 端口配置模式	no 命令为关闭 ipv6 dhcp snooping 功能

【示例】将 1/1 的 dhcp snoop 功能开启

Tritium(config-if)# ipv6 dhcp snooping

7.2.2.2. 设置 dhcp snoop 受信端口

该命令用于配置和删除 ipv6 dhcp snooping 受信端口。

表 7–5 配置/删除 ipv6 dhcp snooping 受信端口

命令	命令模式	功能说明
ipv6 dhcp snooping trust	以太网端口配置模式	设置 ipv6 dhcp snooping 受信端口
no ipv6 dhcp snooping trust	以太网端口配置模式	no 命令为删除 ipv6 dhcp snooping 受信端口

【示例】将端口 1/2 设置为 ipv6 dhcp snooping 受信端口

Tritium(config-if)# ipv6 dhcp snooping trust

7.2.2.3. 显示 ipv6 dhcpsnoop database 配置信息

该命令用于显示 ipv6 dhcpsnoop database 的配置信息。

表 7–6 显示 ipv6 dhcp snooping 配置信息

命令	命令模式	功能说明
show ipv6 dhcpsnoop database	特权用户模式	显示 ipv6 dhcp snoop 配置信息

【示例】显示 dhcp snoop 的配置信息

Tritium# show ipv6 dhcpsnoop database

第 8 章 MAC 配置

8.1. MAC 配置简介

MAC 配置功能主要是维护和 mac 地址学习转发相关的配置和地址信息，能够通过命令配置查看诸如静态地址，动态地址，转发表老化时间，开关学习功能等功能。

8.2.MAC 的配置任务

8.2.1.MAC 的基本配置

8.2.1.1. 配置转发表项

该命令用于配置转发表项。**no** 命令删除指定转发表项。

表 8–1 配置转发表项

命令	命令模式	功能说明
mac-address { **static** | **dynamic** } *mac-address* { **fastethernet** | **gigabitethernet** |10 **gigabitethernet** | **trunk** } *slot/port* { **vlan-id** *vlan-id* | **vlan-name** *vlan-name* }	全局配置模式	配置转发表项。
no mac-address { **static** | **dynamic** } *mac-address* [**vlan-id** *vlan-id* | **vlan-name** *vlan-name*]	全局配置模式	删除指定转发表项。
no mac-address { **static** | **dynamic** | **all** }	全局配置模式	删除指定类型的转发表项。

参数说明：

mac-address：添加的转发表的 MAC 地址。

slot：此 MAC 地址对应的接口板的 slot-num。

port：此 MAC 地址对应的接口板的 port-num。

vlan-id：此 MAC 地址所属于的 VLAN 的 ID。（1~4094）。

vlan-name：此 MAC 地址所属于的 VLAN 的名字。（字符串长度为 1~14）。

【示例】设置 00:00:00:00:11:22 从 VLAN 2 的 1/3 转发。

Tritium(config)# mac-address static *00:00:00:00:11:22* **fastethernet** *1/3* **vlan-id** *2*

8.2.1.2. 配置老化时间

该命令用于配置转发表项的老化时间。**no** 命令恢复转发表项老化时间的缺省值。

表 8–2 配置转发表项的老化时间

命令	命令模式	功能说明
mac-address timer age-timer *time-value*	全局配置模式	配置转发表项的老化时间。
no mac-address timer age-timer	全局配置模式	恢复转发表项老化时间的缺省值。

参数说明：

time-value：添加的转发表的 MAC 地址。缺省情况下为 300 秒。

【示例】设置转发表项的老化时间为 1 分钟。

Tritium(config)# mac-address timer age-timer *60*

8.2.1.3. 禁止 MAC 学习功能

该命令用于 MAC 地址学习功能。**no** 命令恢复 MAC 地址学习功能。缺省情况下允许地址学习。

表 8–3 配置 MAC 地址学习功能

命令	命令模式	功能说明
mac-learning disable	接口配置模式	禁止 MAC 地址的学习功能
no mac-learning disable	接口配置模式	恢复 MAC 地址的学习功能

【示例】禁止当前接口进行地址学习。

Tritium(config-if)# mac-learning disable

8.2.2. 监控和维护 MAC 配置

在完成上述配置后，执行 **show** 命令可以查看 MAC 配置的信息，验证配置的效果。

表 8–4 监控和维护 MAC 配置

命令	命令模式	功能说明
show mac-address { **static** | **dynamic** | **all** }	特权用户模式	查看已经配置静态或者动态转发表项。
show mac-address { **vlan-id** *vlan-id* | **vlan-name** *vlan-name* }	特权用户模式	根据 VLAN ID 或者 VLAN NAME 查看已配置的转发表项。

参数说明：

vlan-id t：该 VLAN 的 ID。（1~4094）。

vlan-name：该 VLAN 的名字。（字符串长度为 1~14）。

【示例】查看已经配置的所有 MAC 信息。

```
Tritium# show mac-address all
mac age-timer: 600 second
mac count:2
============fwd table============
mac-address dynamic 00:00:00:00:00:29 fastethernet 1/1 vlan 1
mac-address static 00:00:00:00:11:22 fastethernet 1/3 vlan 2
```

第 9 章 交换机控制

9.1. 风暴控制

9.1.1. 风暴控制简介

风暴控制是指在网络的广播或者组播流量超过用户设置的值后，系统将对广播/组播流量作丢弃处理，使广播/组播流量所占的带宽降低到合理的范围，从而有效抑制风暴，避免网络拥塞，保证网络业务的正常运行。

9.1.2. 风暴控制的配置任务

9.1.2.1. 配置广播/组播风暴抑制

该命令用于配置广播/组播风暴抑制。

表 9–1 配置广播/组播风暴抑制

命令	命令模式	功能说明
stormcontrol { **broadcast** | **multicast** | **dlf** } **bandwidth** *bandwidthvalue*	以太网接口配置模式/全局配置模式	配置广播/组播风暴抑制。
no stormcontrol { **broadcast** | **multicast** | **dlf** }	以太网接口配置模式/全局配置模式	禁止广播/组播风暴抑制。

参数说明：

bandwidthvalue：端口带宽数值抑制。100M 接口下取值为: <100,100000> pps ，1G 接口下取值为: <100,1000000> pps ， 10G 接口下取值为: <100,10000000>pps，全局下 stormcontrol 取值为: <100,1000000> pps

【适用范围】：

三层交换：支持 dlf 风暴控制。

S3528 系列：bandwidthvalue 的范围为 100－100000pps。

S5324 系列：bandwidthvalue 的范围为 100－1000000pps。

S8508 系列：bandwidthvalue 的范围为 100－1000000pps。

路由，安全平台系列产品：不支持 dlf 风暴控制。

【示例 1】在以太网接口 1/3 上配置广播风暴抑制，抑制速率为 1024pps。

Tritium(config)# interface gigabitethernet *1/3*

Tritium(config-if)# stormcontrol broadcast bandwidth *1024*

【示例 2】在以太网接口 1/8 上配置组播风暴抑制，抑制速率为 2048pps。

Tritium(config)# interface gigabitethernet *1/8*

Tritium(config-if)# stormcontrol broadcast bandwidth *2048*

9.1.2.2. 监控和维护风暴抑制

在完成上述配置后，执行 **show** 命令可以查看风暴抑制的运行信息，验证配置的效果。

表 9–2 监控和维护风暴抑制

命令	命令模式	功能说明
show stormcontrol [**{ fastethernet | gigabitethernet }** *slot/port*]	特权用户模式	查看已经配置的广播/组播风暴抑制的配置信息

参数说明：

slot/port：接口号。

【示例】查看接口 1/8 上已经配置的广播风暴抑制的配置信息。

Tritium# show stormcontrol gigabitethernet *1/8*

broadcast storm control : 1024 pps

9.2. MAC ACL

9.2.1.MAC ACL 简介

9.2.1.1. MAC 访问控制列表概述

MAC 访问控制列表（Access Control Lists）也称为 MAC 访问列表（Access List），它能为所有 MAC 进行配置，交换机会对通过的数据包进行过滤。通过在交换机上配置访问列表可以控制对网络的访问：访问列表能够禁止输入或输出网络的某些流量。

9.2.1.2. MAC 访问列表的作用

MAC 访问列表通过在交换机的接口上控制是否转发或阻止数据包来过滤网络流量。交换机检查每个数据包并基于访问列表中指定的规则来决定是否转发或丢弃这个包。

9.2.1.3. 配置 MAC 访问列表的原因

配置 MAC 访问列表有很多原因，例如，可以通过使用访问列表限制 MAC 更新内容或提供流量控制，但其中最重要的一个原因是要通过配置 MAC 访问列表来提供网络安全性。

应该使用 MAC 访问列表为网络访问提供一个基础层次的安全性，如果在网络的交换机上没有配置访问列表，则所有通过交换机的包将被允许进入网络的每个部分。例如，MAC 访问列表可以允许一台主机访问网络的某一部分，同时阻止另一台主机访问这一区域。

也可以使用 MAC 访问列表决定在交换机接口的何种类型的流量被转发或阻止。

9.2.1.4. MAC 访问控制列表的类别

Tritium 交换机的 MAC 访问控制列表类别为通过名字引用的扩展访问控制列表。

9.2.2.MAC ACL 的配置

9.2.2.1. 配置一条条目

表 9–3 配置/删除一条条目

命令	命令模式	功能说明
{ **deny** | **permit** } { **any** | **host** *src-MAC-addr* | *src-MAC-addr mask* } { **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask* } [**aarp** | **appletalk** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **mumps** | **netbios** | **vines-echo** | **xns-idp** | { *ethernt-type* [*ethernt-mask*] }] [**sequence** *sequence-number*]	MAC 访问控制列表配置模式	创建一条条目。
no { **deny** | **permit** } { **any** | **host** *src-MAC-addr* | *src-MAC-addr mask* } { **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask* } [**aarp** | **appletalk** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **mumps** | **netbios** | **vines-echo** | **xns-idp**| { *ethernt-type* [*ethernt-mask*] }]	MAC 访问控制列表配置模式	删除一条条目。
no sequence *sequence-number*	MAC 访问控制列表配置模式	根据序号删除一条条目。

参数说明：

src-MAC-addr：源 MAC 地址，格式为 aa:bb:cc:dd:ee:ff，如 00:01:98:7c:ff:62。

dst-MAC-addr：目的 MAC 地址，格式为 aa:bb:cc:dd:ee:ff。

ethernt-type：以太类型，取值 1536~65535，如 IP 类型码是 0x0800，arp 是 0x0806。

ethernt-mask：以太类型掩码，取值 0~65535，不指定默认为 65535。

aarp：AppleTalk ARP，ethernet-type = 0x80F3。

appletalk：AppleTalk/EtherTalk，ethernet-type=0x809B。

decnet-iv：DECnet Phase IV，ethernet-type=0x6003。

diagnostic：DEC-Diagnostic，ethernet-type=0x6005。

dsm：DEC-DSM，ethernet-type=0x8039。

etype-6000：ethernet-type = 0x6000。

etype-8042：ethernet-type=0x8042。

lat：DEC-LAT，ethernet-type=0x6004。

lavc-sca：DEC-LAVC-SCA，ethernet-type=0x6007。

mop-console：DEC-MOP Remote Console，ethernet-type=0x6002。

mop-dump：DEC-MOP Dump，ethernet-type=0x6001。

mumps：DEC-MUMPS，ethernet-type=0x6009。

netbios：DEC-NETBIOS，ethernet-type=0x8040。

vines-echo：VINES Echo，ethernet-type=0x0BAE。

xns-idp：XNS IDP，ethernet-type=0x0600。

sequence-number：条目的序列号，取值 1～2147483647。

【示例】添加一条允许从 MAC 地址 00:01:34:56:7a:12 到所有地址的 IP 报文的规则。

Tritium(config-ext-macl)# permit *00:01:34:56:7a:12 00:00:00:00:00:00* any *2048 65535*

9.2.2.2. 配置对进入的报文进行过滤

表 9–4 配置对进入的报文进行过滤

命令	命令模式	功能说明
mac access-group *name* **in**	接口配置模式	从该接口进入的报文进行过滤。
no mac access-group in	接口配置模式	禁止对从该接口进入的报文进行过滤。

参数说明：

name：引用的 MAC 访问控制列表的名字。

【示例 1】在某二层接口上使用名字为 abc 的 MAC 访问控制列表进行过滤。

Tritium(config-if)# mac access-group *abc* **in**

【示例 2】在某二层接口上取消 MAC 访问控制列表的过滤。

Tritium(config-if)# no mac access-group in

9.2.2.3. 创建一组 mac access-list

表 9–5 创建一组 mac access-list

命令	命令模式	功能说明
mac access-list extended *name*	全局配置模式	创建一组 mac access-list，并进入 MAC 访问控制列表配置模式。
no mac access-list extended *name*	全局配置模式	删除一组 mac access-list。

参数说明：

name：MAC 列表的名字

【示例 1】创建名字为 abc 的 MAC 列表。

Tritium(config)# mac access-list extended *abc*

9.2.2.4. 重新设置一个 MAC 访问控制列表的所有条目的序列号

表 9–6 重新设置一个 MAC 访问控制列表的所有条目的序列号

命令	命令模式	功能说明
mac access-list resequence *mac-acl-name start-number step-number*	全局配置模式	重新设置一个 MAC 访问控制列表的所有条目的序列号。

参数说明：

mac-acl-name：MAC 访问控制列表名称。

start-number：起始序号，缺省为 10。

step-number：序号步长，缺省为 10。

【示例】对 MAC 访问控制列表 abc，从 10 开始重新设置序列号，序号增加的步长为 20。

Tritium(config)# mac access-list resequence *abc 10 20*

设置前：

Extended MAC access list abc(4 entry)

10 permit host 00:01:23:45:67:01 any 32768

20 permit host 00:01:23:45:67:01 any 2054

30 permit host 00:01:23:45:67:02 any 32768

40 permit host 00:01:23:45:67:02 any 2054

设置后：

Extended MAC access list abc (4 entry)

10 permit host 00:01:23:45:67:01 any 32768

30 permit host 00:01:23:45:67:01 any 2054

50 permit host 00:01:23:45:67:02 any 32768

70 permit host 00:01:23:45:67:02 any 2054

mac access-list resequence abc 10 20

9.2.2.5. 根据序号删除一条条目

表 9–7 根据序号删除一条条目

命令	命令模式	功能说明
no sequence *sequence-number*	MAC 访问控制列表配置模式	根据序号删除一条条目。

参数说明：

sequence-number：条目的序列号，取值 1～2147483647。

【示例】删除序号为 10 的条目。

Tritium(config-ext-macl)# no sequence *10*

9.2.2.6. 监控和维护 MAC 列表

表 9–8 监控和维护 MAC 列表

命令	命令模式	功能说明
show mac access-list [*name*]	特权用户模式	显示一组或所有 MAC 列表。

参数说明：

name：MAC 访问控制列表的名字，如果不指定则显示所有。

【示例】显示名字为 abc 的 MAC 访问控制列表。

Tritium# show mac access-list *abc*

```
Extended MAC access list abc(4 entry).
    10 permit host 00:01:23:45:67:01 any 32768
    20 permit host 00:01:23:45:67:01 any 2054
    30 permit host 00:01:23:45:67:02 any 32768
    40 permit host 00:01:23:45:67:02 any 2054
```

9.3. 端口镜像

适用平台：bcm 平台，5000 系列交换机，8000 系列交换机

9.3.1.端口镜像简介

端口镜像（Port Mirroring）可以让用户将所有的流量从一个特定的端口复制到一个镜像端口。

如果提供端口镜像功能，则允许管理人员自行设置一个监视管理端口来监视被监视端口的数据。监视到的数据可以通过 PC 上安装的网络分析软件来查看，通过对数据的分析就可以实时查看被监视端口的情况。

9.3.2.端口镜像的配置

9.3.2.1. 使能/禁止端口镜像

该命令用于使能/禁止端口镜像,缺省情况下 mirror 功能是 disable。

表 9–9 使能/禁止端口镜像

命令	命令模式	功能说明
mirror { **enable** | **disable** }	全局配置模式	使能/禁止端口镜像。

【示例 1】使能端口镜像。

Tritium(config)# mirror enable

9.3.2.2. 配置端口镜像

该命令用于配置端口镜像。

表 9–10 使能/禁止端口镜像

命令	命令模式	功能说明
mirror *slot-list/port-list* **mirror-type** *src-type* **target-port** *slot/port*	全局配置模式	配置端口镜像。

参数说明：

slot-list：端口镜像板子的 slot 集合，通过“/”隔离。

port-list：端口镜像的 port 的集合，通过“,”连接。

slot-list/port-list 格式如：1/1,1/2,2/1,2/2,3/1，一次最多允许配置 4 个端口。

src-type：端口镜像的类型，有 both，ingress，egress3 种。

slot/port：端口镜像目的端口的 slot 号和 port 号。

【示例】将 1/1,1/2,1/3 端口的 ingress 和 egress 端数据镜像到接口 1/6。

Tritium(config)# mirror *1/1, 1/2, 1/3* **mirror-type both target-port** *1/6*

9.3.2.3. 配置远程端口镜像

该命令用于配置 RSPAN。

表 9–11 配置远程端口镜像

命令	命令模式	功能说明
mirror *slot-list/port-list* **mirror-type** *src-type* **reflector-port** *slot/port* **remote-vlan** *vlan-id*	全局配置模式	配置远程端口镜像。

参数说明：

slot-list：端口镜像板子的 slot 集合，通过“/”隔离。

port-list：端口镜像的 port 的集合，通过“,”连接。

slot-list/port-list 格式如：1/1,1/2,2/1,2/2,3/1，一次最多允许配置 4 个端口。

src-type：端口镜像的类型，有 both，ingress，egress3 种。

slot/port：反射端口的 slot 号和 port 号。

Vlan-id：Probe remote vlan-id,用于传输远程镜像报文。

【示例】将 1/2,1/3 端口的 ingress 和 egress 端数据镜像到远程 vlan 50。

Tritium(config)# mirror *1/2, 1/3* **mirror-type both reflector-port** *1/4* **remote-vlan** *50*

9.3.2.4. 配置 vlan 端口镜像

该命令用于配置 vlan mirror

表 9–12 配置 vlan 端口镜像

命令	命令模式	功能说明
mirror vlan *vid* **mirror-type [***ingress*	*egress***] target-port** *slot/port*	全局配置模式	配置 vlan 端口镜像。

参数说明：

Vlan：端口镜像源 vlan id。

mirror-type：端口镜像的类型，有 ingress，egress 2 种。

slot/port：目的端口的 slot 号和 port 号。

【示例】将 vlan 10 的 ingress 端数据镜像到目的端口 1/5。

Tritium(config)# mirror vlan *10* **mirror-type** *ingress* **target-port** *1/5*

9.3.2.5. 配置 acl 端口镜像

该命令用于配置 acl mirror

表 9–13 配置 acl 端口镜像

命令	命令模式	功能说明
mirror access-group [*acl-id* | *acl-name***] mirror-type [***ingress* | *egress***] target-port** *slot/port*	全局配置模式	配置 acl 端口镜像。

参数说明：

Access-group：端口镜像源 access-group id。

mirror-type：端口镜像的类型，有 ingress，egress 2 种。

slot/port：目的端口的 slot 号和 port 号。

【示例】将 access-group 10 的 ingress 端数据镜像到目的端口 1/5。

Tritium(config)# mirror access-group *10* **mirror-type** *ingress* **target-port** *1/5*

9.3.2.6. 监控和维护端口镜像

该命令用于显示端口镜像配置信息。

表 9–14 使能/禁止端口镜像

命令	命令模式	功能说明
show mirror	特权用户模式	显示端口镜像配置信息。

第 10 章 PVLAN

10.1. PVLAN (Primary-VLAN)

10.1.1. PVLAN 概述

10.1.1.1. PVLAN 背景

VLAN最初是一种虚拟工作组概念，是在同一个交换机上面，实现不同工作组之间的隔离，共享一个交换机设备。引入PVLAN这样的组网方式，实现了接入用户二层报文的隔离，保证了安全性。同时上层交换机下发的报文可以被每一个用户接收到，简化了配置，并且由于PVLAN对于三层交换机来说是不可见的，节省了交换网络中的VLAN资源。

10.1.2. PVLAN 配置

10.1.2.1. 配置 PVLAN 类型

在 vlan 配置模式下配置 pvlan 类型为 primary 或 secondary。

表 10–1 配置 pvlan 类型

命令	命令模式	功能说明
pvlan-type {primary | secondary}	vlan 配置模式	选择 pvlan 类型

10.1.2.2. 配置 PVLAN MAP

配置 pvlan 主次 vlan 间映射关系。

表 10–2 配置 pvlan map

命令	命令模式	功能说明
Pvlan mapping primary *vlan-id* **secondary** *vlan-id*	全局配置模式	配置主次 vlan 映射关系。
No Pvlan mapping primary *vlan-id* **secondary** *vlan-id*	全局配置模式	解除主次 vlan 映射关系。

10.1.2.3. 显示 PVLAN MAP

表 10–3 显示 pvlan map

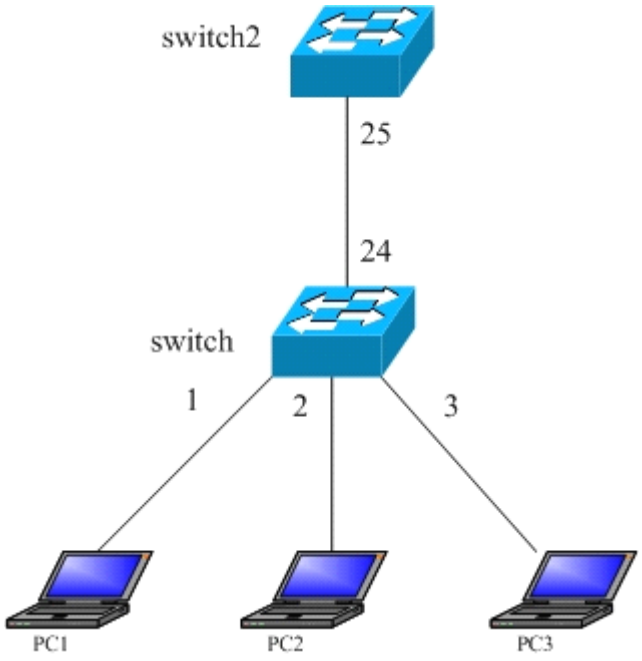
命令	命令模式	功能说明
Show pvlan map	特权模式	显示所有主次 vlan 的映射关系。

10.1.3. PVLAN 配置实例

10.1.3.1. 组网需求

PC1,PC2,PC3 之间互相隔离,都可以通过 port 24 与外界通信.

10.1.3.2. 组网图



10.1.3.3. 配置步骤

（1） 配置 switch

！创建主 vlan。

Tritium(config)# vlan 100

Tritium(config-vlan)# pvlan-type primary

Tritium(config-vlan)# port *1/24* untagged

Tritium(config)# interface 10gigabitethernet *1/24*

Tritium(config-if)# switchport pvid *100*

！创建次 vlan。

Tritium(config)# vlan 11

Tritium(config-vlan)# pvlan-type secondary

Tritium(config-vlan)# port *1/1* untagged

Tritium(config)# interface gigabitethernet *1/1*

Tritium(config-if)# switchport pvid *11*

Tritium(config)# vlan 12

Tritium(config-vlan)# pvlan-type secondary

Tritium(config-vlan)# port *1/2* untagged

Tritium(config)# interface gigabitethernet *1/2*

Tritium(config-if)# switchport pvid *12*

Tritium(config)# vlan 13

Tritium(config-vlan)# pvlan-type secondary

Tritium(config-vlan)# port *1/3* untagged

Tritium(config)# interface gigabitethernet *1/3*

Tritium(config-if)# switchport pvid *13*

！建立主次 vlan 映射关系。

Tritium(config)# pvlan mapping primary 100 secondary 11

Tritium(config)# pvlan mapping primary 100 secondary 12

Tritium(config)# pvlan mapping primary 100 secondary 13

（2） 配置 Switch2

！创建 vlan 100。

Tritium(config)# vlan 100

！向 vlan 100 添加端口。

Tritium(config-vlan)# port *1/25* untagged

！配置 pvid。

Tritium(config)# interface 10gigabitethernet *1/25*

Tritium(config-if)# switchport pvid *100*

第 11 章 802.1x

11.1. 802.1x

11.1.1.802.1x 简介

802.1x 协议是作为局域网端口的一个普通接入控制机制用在以太网中，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制（Port Based Network Access Control）协议。在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源—相当于连接被物理断开。

IEEE 802.1x 的体系结构中包括三个部分：

Supplicant System：用户接入设备；

Authenticator System：接入控制单元；

Authentication Server System：认证服务器；

在用户接入层设备如 LANSWITCH 实现 802.1x 的认证系统部分，即 Authenticator 802.1x 的客户端一般安装在用户 PC。典型为 Windows XP 操作系统自带的客户端 802.1x 的认证服务器系统一般驻留在运营商的 AAA 中心。

Supplicant 与 Authenticator 间运行 IEEE802.1X 定义的 EAPOL 协议；Authenticator 与 Authentication Server 间同样运行 EAP 协议，EAP 帧中封装了认证数据，将该协议承载在其它高层次协议中，如 Radius，以便穿越复杂的网络到达认证服务器 EAP Relay。

Authenticator 每个物理端口内部有受控端口 Controlled Port 和非受控端口 unControlledPort。非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议。非受控端口可保证随时接收 Supplicant 发出的认证 EAPOL 报文，受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控仅输入受控两种方式以适应不同的应用环境。

11.1.2.802.1x 配置

11.1.2.1. 使能/禁止 802.1x

802.1x 缺省情况下是禁止的。

表 11–1 使能/禁止 802.1x

命令	命令模式	功能说明
802.1x *slot/port-list*	全局配置模式	使能指定接口的 802.1x
no 802.1x *slot/port-list*	全局配置模式	禁止指定接口的 802.1x

参数说明：

slot/port-list：接口号，类似 1/1-9，18，以“，”“-”连接的 port 号。

11.1.2.2. 配置 802.1x macbind

缺省情况未绑定，允许任何用户认证，一旦绑定了 mac 地址，就只允许绑定了的 mac 地址进行认证接入。一个接口可以绑定多个 mac 地址。

表 11–2 使能/禁止 802.1x

命令	命令模式	功能说明
802.1x *slot/port-list* **macbind** *mac-address*	全局配置模式	将端口与特定 mac 地址绑定
no 802.1x *slot/port-list* **macbind** *mac-address*	全局配置模式	解除端口与特定 mac 地址的绑定

参数说明：

slot/port-list 类似 1/1-9,18,以”,”,”-“连接的 port 号

mac-address 允许认证的 mac 地址

11.1.2.3. 配置 802.1x 重认证

本命令用于使能/禁止 802.1x 重认证。

表 11–3 使能/禁止 802.1x 重认证

命令	命令模式	功能说明
802.1x re-authenticate	全局配置模式	使能所有接口的重认证
no 802.1x re-authenticate	全局配置模式	关闭所有接口的重认证

参数说明：

无

11.1.2.4. 配置 802.1x 重认证周期

本命令用于配置/恢复 802.1x 重认证周期。

表 11–3 配置/恢复 802.1x 重认证

命令	命令模式	功能说明
802.1x re-authenticate time *times-value*	全局配置模式	配置重认证周期同时开启接口重认证机制
no 802.1x re-authenticate time	全局配置模式	恢复重认证周期至默认值

参数说明：

times-value：设置重认证周期。时间从最近一次成功认证算起，范围是 1~65535 秒，缺省值为 3600 秒。

11.1.2.5. 配置 802.1x 的报文重传次数

表 11–4 配置 802.1x 的报文重传次数

命令	命令模式	功能说明
802.1x retry *times-value*	全局配置模式	配置 802.1x 的报文重传次数
no 802.1x retry	全局配置模式	恢复报文重传次数至默认值

参数说明：

times-vlaue：重传时间值，范围为 1~65535 次，缺省值为 2 次。

11.1.2.6. 配置 802.1x 的计数值

表 11–5 配置 802.1x 的计数值

命令	命令模式	功能说明
802.1x timer {quiet-period *quiet-period time-value* | **tx-period** *tx-period time-value* | **supp-timeout** *supp-timeout time-value*| **server-timeout** *server-timeout time-value***}**	全局配置模式	配置协议相关计数值信息
no 802.1x timer {quiet-period time-value | tx-period time-value | supp-timeout	全局配置模式	恢复协议相关计数值信息至默认值。

time-value | server-timeout time-value }		

参数说明：

quiet-period : 配置静默时间后，当用户终端收到从认证服务器传来的拒绝该用户的接入请求报文后，在此时间间隔内，不论用户采取任何手段与服务器联系，系统将保持静默不予理睬。

注意：*quiet-period* 参数只适用于单用户，多用户不支持

quiet-period time-value: 范围是 1～65535 秒，缺省值为 60 秒

tx-period: 配置认证系统向客户端重传 EAP-Request/Identity 数据帧的时间间隔.

tx-period time-value: 范围是 1～65535 秒，缺省值为 30 秒

supp-timeout: 配置接收来自客户端的报文的超时时间

supp-timeout time-value: 范围是 1～65535 秒，缺省值为 30 秒

server-timeout: 配置接收来自认证服务器的报文的超时时间

server-timeout time-value: 范围是 1～65535 秒，缺省值为 30 秒

11.1.2.7. 配置接口的认证状态

表 11–6 配置接口的认证状态

命令	命令模式	功能说明
802.1x control { **auto** | **authorized-force** | **unauthorized-force** } *slot/port-list*	全局配置模式	配置接口的认证状态
no 802.1x control *slot/port-list*	全局配置模式	恢复接口的认论状态至默认值

参数说明：

auto：此时端口处于接受认证状态，用户能否访问网络完全取决于用户能否认证成功。此配置为缺省值。

authorized-force：此时端口无条件的处于已授权状态，用户可以访问网络。

unauthorized-force：此时端口无条件的处于未授权状态，用户不能访问网络。

slot/port-list ：接口号，类似 1/1-9,18,以”,”,”-“连接的 port 号

11.1.2.8. 配置 802.1x 的计费功能

表 11–7 配置 802.1x 的计费功能

命令	命令模式	功能说明
802.1x accounting *slot/port-list*	全局配置模式	使能计费功能。
no 802.1x accounting *slot/port-list*	全局配置模式	禁止计费功能。

参数说明：

slot/port-list：接口号，类似 1/1-9,18,以”,”,”-“连接的 port 号

11.1.3.802.1x 的监控与维护

表 11–8 802.1x 的监控与维护

命令	命令模式	功能说明
show 802.1x *slot/port-list*	特权用户模式	显示端口 802.1x 的配置。
show 802.1x user_message *slot/port*	特权用户模式	查看接口下用户认证信息。

参数说明：

slot/port-list：接口号，类似 1/1-9,18,以”,”,”-“连接的 port 号.

11.1.4.Radius-sever 配置

表 11–9 802.1x 的监控与维护

命令	命令模式	功能说明
802.1x radius-server vid {*vid*} **key** {*share-key*} {**ipv4** *ipv4-address*| **ipv6** *ipv6-addrss*}	全局用户模式	配置 802.1x RADIUS 服务器

参数说明；

{*vid*}:指定管理 VLAN。

{*share-key*}:传递的报文都是使用加密算法进行确认的，在 radius server 和 radius client 间的使用共享密钥 share-key，采用 md5 算法计算报文的 hash 值。

{**ipv4** *ipv4-address*}:认证用户的 radius 服务器的 IPv4 地址，格式为：x.x.x.x

{**ipv6** *ipv6-address*}:认证用户的 radius 服务器的 IPv6 地址，格式为：x:x:x:x::x/<0-128>

11.1.5.802.1x 配置举例

使能接口 1/1~1/3 的 802.1X，并配置 Radius Server 为 192.168.0.1，共享密钥为 Radius

！使能端口 1/1~1/3 的 802.1x

Tritium(config)# 802.1x *1/1-3*

！配置 Radius Server 为 192.168.0.1，共享密钥为 Radius ，管理 vlan 为 1

Tritium(config)# 802.1x radius-sever vid *1* **key Radius ipv4** *192.168.0.1*

11.2. 配置 802.1x 的 keepalive 功能

11.2.1. 开启/关闭接口 802.1x keepalive 功能

表 11–10 配置/恢复 802.1x 重认证

命令	命令模式	功能说明
802.1x keepalive *slot/port*	全局配置模式	开启接口 802.1x keepalive 功能
no 802.1x keepalive *slot/port*	全局配置模式	关闭接口 802.1x keepalive 功能

参数说明：

slot/port：接口号，类似 1/1。

11.2.2. 配置发送 keepalive 间隔时间

表 11–11 配置/恢复 802.1x keepalive 参数

命令	命令模式	功能说明
802.1x keepalive interval-time *time-value*	全局配置模式	配置发送 keepalive 间隔时间
no 802.1x keepalive interval-time *time-value*	全局配置模式	恢复发送 keepalive 间隔时间为默认值

参数说明：

time-value：整型数。

11.2.3. 配置 keepalive 超时重传次数

表 11–12 配置/恢复 802.1x keepalive 超时重传次数

命令	命令模式	功能说明
802.1x keepalive retrans-times *times-value*	全局配置模式	配置发送 keepalive 报文的超时重传次数
no 802.1x keepalive retrans-times *times-value*	全局配置模式	恢复发送 keepalive 报文的超时重传次数为默认值

参数说明：

Times-value：整型数

11.3. 802.1x accounting update 功能

11.3.1. 开启/关闭接口 802.1x 计费 update 功能

表 11–13 配置/恢复 802.1x 计费 update

命令	命令模式	功能说明
802.1x accounting update enable port *slot/port-list*	全局配置模式	开启接口 802.1x 计费 update 功能
no 802.1x accounting update enable port *slot/port-list*	全局配置模式	关闭接口 802.1x 计费 update 功能

参数说明：

slot/por-listt：接口号，类似 1/1，10-15。

11.3.2. 配置发送计费 update 间隔时间

表 11–14 配置/恢复 802.1x 计费 update 参数

命令	命令模式	功能说明
802.1x accounting update interval-time *time-value*	全局配置模式	配置发送计费 update 间隔时间
no 802.1x accounting update	全局配置模式	恢复发送计费 update 间隔时间为

interval-time *time-value*		默认值

参数说明：

time-value：整型数。

11.3.3. 配置计费 update 超时重传次数

表 11–15 配置/恢复 802.1x 计费 update 超时重传次数

命令	命令模式	功能说明
802.1x accounting update retrans-times *times-value*	全局配置模式	配置发送计费 update 报文的超时重传次数
no 802.1x accounting update retrans-times *times-value*	全局配置模式	恢复发送计费 update 报文的超时重传次数为默认值

参数说明：

Times-value：整型数

11.4. 802.1X 新增特性

11.4.1. 自动注销

使能自动注销后，对认证成功接口，如果在规定时间内无数据流动，即 in 或者 out 方向数据流动字节数为 0，则自动注销该接口上用户。默认情况下禁止自动注销。

表 11–16 使能/禁止 802.1x 自动注销

命令	命令模式	功能说明
802.1x auto-logoff port *slot/port*	全局配置模式	使能指定接口的 802.1x 自动注销
no 802.1x auto-logoff port *slot/port*	全局配置模式	禁止指定接口的 802.1x 自动注销
802.1x auto-logoff time *<10-65535>*	全局配置模式	配置接口的自动注销时间
no 802.1x auto-logoff time	全局配置模式	恢复接口的自动注销时间为默认值

参数说明：

slot/port-list：接口号，类似 1/1-9，18，以"，""-"连接的 port 号。

<10-65535> ： 接口自动注销时间，默认为 600 秒。

11.4.2. 802.1x 的 log

用于记录非用户主动退出时信息供管理员查看。

表 11–17 配置 log 的条数

命令	命令模式	功能说明
802.1x log-message counter *<0-100>*	全局配置模式	配置 log 的条数
no 802.1x log-message counter	全局配置模式	恢复 log 的条数为默认值
show 802.1x log-message	特权模式	查看 log 消息

参数说明：

<0-100> ： 允许记录的 log 条数。默认值为 50

第 12 章 Rmon

12.1. rmon

12.1.1. RMON 概述

远程监控（RMON）是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由 SNMP MIB 扩展而来。RMON 中，网络监视数据包含了一组统计数据和性能指标，它们在不同的监视器（或称探测器）和控制台系统之间相互交换。结果数据可用来监控网络利用率，以用于网络规划，性能优化和协助网络错误诊断。

当前 RMON 有两种版本：RMON v1 和 RMONv2。RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMON v2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。

RMON 监视系统有两部分构成：探测器（代理或监视器）和管理站。RMON 代理在 RMON MIB 中存储网络信息，它们被直接植入网络设备（如路由器、交换机等），代理也可以是 PC 机上运行的一个程序。代理只能看到流经它们的流量，所以在每个被监控的 LAN 段或 WAN 链接点都要设置 RMON 代理，网管工作站用 SNMP 获取 RMON 数据信息。

RMON MIB 有不少变种。例如，令牌网 RMON MIB 提供了针对令牌网网络管理的对象。SMON MIB 是由 RMON 扩展而来，主要用来为交换网络提供 RMON 分析。

RMON 定义

RMON 共包含 7 个组，目前支持了四个组。

Event Group: 控制在此处事件的产生和报告。其元素包括：事件类型、描述、事件最后一个发送的时间

Alarm Group: 定期从探测器的变量选取统计例子。并与前面配的阈值相比较。其元素包括：告警类型、间隔、阈值上限、阈值下限

Statistics Group: 包括探测器为该设备每个监控的接口测量的统计值。其元素包括：数据包丢弃、数据包发送、广播数据包、CRC 错误、大小块、冲突以及计数器的数据包。范围从 65~127、128~255、256~511、512~1023 以及 1024~1518 字节。

History Group: 定期地收集统计网络值地记录并存储起来以便日后提取。其元素包括：取样周期、样品数目和项目。提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

12.1.2. RMON 配置

12.1.2.1. 配置/删除/查看 event 组

表 12–1 配置/删除/查看 event 组

命令	命令模式	功能说明
rmon event *event-entry* [**description** *string*] {**log**| **trap** *trap-community* |**log-trap** *log-trapcommunity* | **none**} [**owner** *config*]	全局配置模式	配置 RMON Event 表项
no rmon event *event-entry*	全局配置模式	删除指定 RMON 表项
show rmon event	特权模式	查看 RMON Event 配置

参数说明：

event-entry：添加/删除 event 表项的索引号，取值范围为 1~65535

description *string*:事件的描述，字符串，长度为 1~127 个字符

log：日志事件

trap *trap-community*：Trap 事件，接收事件消息的网管站的团体名属性，字符串，长度为 1~127 个字符。

Log-trap *log-trapcommunity*：定义事件为日志和 Trap 事件，接收事件消息的网

管站的团体名属性，字符串，长度为 1~127 个字符。

None：不产生动作的事件

owner *config*：该表项的创建者，字符串，长度为 1~127 个字符，默认为 config

12.1.2.2. 配置/删除/查看 alarm 组

表 12–2 配置/删除/查看 alarm 组

命令	命令模式	功能说明
rmon alarm <*entry-number*> <*alarm-variable*> <*sampling-time*> {**delta**|**absolute**} **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *config*]	全局配置模式	配置 RMON Alarm 表项
no rmon alarm *entry-number*	全局配置模式	删除指定 RMON 表项
show rmon alarm	特权模式	查看 RMON Alarm 配置

参数说明：

entry-number ：添加/删除 alarm 表项的索引号，范围 1-65535

alarm-variable：告警变量，字符串类型，长度(1-256)，格式为节点 OID 的点分格式，如 1.3.6.1.2.1.2.1.10.1，只有可以解析为 ASN.1 中的 INTERGER，Counter，Gauge 及 TimeTicks 的数据类型的变量才能作为告警变量。

Sampling-time：采样时间间隔，取值范围为 5~65535，单位为秒。

Delta：采样类型为变化值(当前采样值相对于最近一次采样值的变化量)

Absolute：采样类型为当前值。

Rising_threshold *threshold-value1*：上限阈值，取值范围为 0~2147483647

event-entry1 ：上限阈值相对应的事件号，取值范围为 0~65535

falling_threshold *threshold-value2*：下限阈值，取值范围为 2~2147483647

event-entry2：下限阈值相应的事件号，取值范围为 0~65535

owner *config* ：该表项的创建者，字符串，长度为 1~127 个字符，默认为 config

使用指南：

建议在配置 alarm 表项之前先配置其需要的 event 事件，如果 alarm 表项对应的

event 事件不存在，则什么都不做。

12.1.2.3. 配置/删除/查看 statistics 组

表 12–3 配置/删除/查看 statistics 组

命令	命令模式	功能说明
rmon statistics *entry-number* [**owner** *config*]	以太网接口配置模式	配置 RMON Statistics 表项
no rmon statistics *entry-number*	以太网接口配置模式	删除指定 RMON 表项
show rmon statistics	特权模式	查看 RMON Statistics 配置

参数说明：

entry-number： 添加/删除统计表项的索引号，取值范围为 1~65535

owner *config*：统计表项的创建者，字符串，长度为 1~127 个字符，默认为 config

12.1.2.4. 配置/删除/查看 history 组

表 12–4 配置/删除/查看 history 组

命令	命令模式	功能说明
rmon history *entry-num* [**bucket** *number*][**interval** *sampling-interval*] [**owner** *config*]	以太网接口配置模式	配置 RMON History 表项
no rmon history *entry-num*	以太网接口配置模式	删除指定 RMON 表项
show rmon history	特权模式	查看 RMON History 配置

参数说明：

entry-num：添加/删除 history 表项的索引号，取值范围为 1~65535

bucket *number*：该表项所对应的历史表容量。取值范围为 1~65535，默认值为 50

interval *sampling-interval*：采样时间，取值范围为 5~3600，单位为秒，默认值为 1800

owner *config*：该表项的创建者，字符串，长度为 1~127 个字符，默认值为 config

第 13 章 动态 ARP 检查

13.1. 动态 ARP 检查简介

动态 ARP 检查（DAI）是网络中 ARP 报文验证的一个安全特性。DAI 允许网络管理员截取，记录，丢弃 MAC 地址与 IP 地址绑定不合法的 ARP 报文，提供了网络中的恶意攻击防止保障。

13.2. 动态 ARP 检查（DAI）的配置

13.2.1. 配置 ip 与 mac 绑定关系

该命令用于静态的配置客户端的 ip 和 mac 的绑定关系。

表 13–1 配置 ip 和 mac 绑定关系

命令	命令模式	功能说明
ip *x.x.x.x* **mac** *xx:xx:xx:xx:xx:xx* **port** *slot*/*port* **[vlan** *vid***]**	全局配置模式	配置客户端 ip 和 mac 的绑定关系
no ip *x.x.x.x* **mac** *xx:xx:xx:xx:xx:xx* **port** *slot*/*port* **[vlan** *vid***]**	全局配置模式	删除客户端 ip 和 mac 的绑定关系

【示例】静态配置客户端 ip 和 mac 的绑定关系。

Tritium(config)# ip 1.1.1.1 mac 00:11:11:11:11:11 port 1/1 vlan 10

13.2.2. 端口使能 DAI 功能

该命令用于在端口上使能动态 ARP 检查功能.

表 13–2 端口使能 DAI

命令	命令模式	功能说明
arp inspection	端口配置模式	在端口上使能动态 ARP 检查功能

【示例】在端口上使能动态 ARP 检查功能

Tritium(config-if)# arp inspection

13.2.3. 使能 arp 表自动绑定功能

该命令用于使能 arp 表自动绑定功能。

表 13–3 使能 arp 表自动绑定功能

命令	命令模式	功能说明
arp auto-bind enable	全局配置模式	使能 arp 表自动绑定功能

【示例】使能 arp 表自动绑定功能

Tritium(config)# arp auto-bind enable

13.2.4. 使能 arp 冲突检测功能

该命令用于使能 arp 冲突检测功能。

表 13–4 使能 arp 冲突功能

命令	命令模式	功能说明
arp conflict-check enable	全局配置模式	使能 arp 冲突检测功能
no arp conflict-check enable	全局配置模式	关闭 arp 冲突检测功能

【示例】使能 arp 冲突检测功能

Tritium(config)# arp conflict-check enable

13.2.5. 转移冲突 arp 信息到 dai 表里

该命令用于将合法的冲突 arp 信息转移到 dai 表里。

表 13–5 转移冲突 arp 信息到 dai 表里

命令	命令模式	功能说明
arp conflict-check transfer	全局配置模式	转移冲突 arp 信息到 dai 表里

【示例】开启转移冲突 arp 信息到 dai 表里功能

Tritium(config)# arp conflict-check transfer

13.2.6. 删除 arp 绑定信息

该命令用于删除 arp 绑定信息。

表 13–6 删除 arp 绑定信息

命令	命令模式	功能说明
no ip arp inspection { admin | dynamic | static }	全局配置模式	删除 arp 绑定信息

【示例】删除静态 arp 绑定信息

Tritium(config)# no ip arp inspection static

13.2.7. 显示 dai 信息

该命令用于显示动态 ARP 检查功能的相关信息。

表 13–7 显示 dai 配置关系

命令	命令模式	功能说明
show ip arp inspection [table | conflict-list | interface *{interface-type interface-num}*]	特权用户模式	显示动态 ARP 检查功能的相关信息

【示例】

1. 显示动态 ARP 检查功能配置的客户端 ip 和 mac 的绑定关系

   Tritium# show ip arp inspection table

2. 显示 ARP 冲突信息

   Tritium# show ip arp inspection conflict-list

3. 显示动态 ARP 检查功能端口配置信息

   Tritium# show ip arp inspection interface fastethernet 1/1

第 14 章 邻居发现检测

14.1. ND SNOOP 简介

ND SNOOP 是网络中 ND 报文验证的一个安全特性。ND SNOOP 允许网络管理员截取，记录，丢弃 MAC 地址与 IPv6 地址绑定不合法的 ND 报文，提供了网络中的恶意攻击防止保障。

14.2. ND SNOOP 的配置

14.2.1. 使能 ND SNOOP

该命令用于使能指定接口的 nd snoop

表 14–1 使能 nd snoop 功能

命令	命令模式	功能说明
ipv6 nd snoop enable	以太网接口配置模式	使能 nd snoop 功能
no ipv6 nd snoop enable	以太网接口配置模式	禁止 nd snoop 功能

【示例】使能接口下的 nd snoop 功能。

Tritium(config-if)# **ipv6 nd snoop enable**

14.2.2. 配置 ipv6 地址与 mac 绑定关系

该命令用于静态配置 ipv6 地址和 mac 的绑定关系

表 14–2 配置 ip 和 mac 绑定关系

命令	命令模式	功能说明
ipv6 *x:::x* **mac** *xx:xx:xx:xx:xx:xx* **port** *slot*/*port* **[vlan** *vid***]**	全局配置模式	静态配置用户 ipv6 和 mac 绑定的命令

【示例】静态配置客户端 ip 和 mac 的绑定关系。

Tritium(config)# ipv6 *01::01* **mac** *00:11:11:11:11:11* **port** *1/1* **vlan** *10*

14.2.3. 显示 nd-snoop 信息

该命令用于显示 ipv6 静态配置绑定信息

表 14–3 显示 nd-snoop 静态配置绑定信息

命令	命令模式	功能说明
show ipv6 nd-snoop [table | interface *{interface-type interface-num}***]**	特权用户模式	显示 nd-snoop 静态配置绑定信息

【示例】

1. 显示静态 nd-snoop 静态配置绑定信息

Tritium# show ipv6 nd-snoop table

2. 显示指定接口的 nd-snoop 静态配置绑定信息

Tritium# show ipv6 nd-snoop interface fastethernet 1/1（3052/3028）

Tritium# show ipv6 nd-snoop interface gigabitethernet 1/1（8500/5328）

第 15 章 环回检测

15.1. Loopdetection 简介

环回检测功能是为了监测交换机的端口是否出现环路。

使能该功能后，交换机会定时发送报文检测接口是否存在环回，如果端口出现环回，且用户未配置手动 shutdown，就将接口 shutdown，禁止接口学习及转发数据；如果用户配置了手动 shutdown，则提示用户出现环回，不自动 shutdown 接口。

15.2. Loopdetection 配置

15.2.1. 使能 loopdetection

使能/关闭某个接口的 loopdetection 功能。

表 15–1 使能 loopdetection

命令	命令模式	功能说明
loop-detection s*lot-list/port-list*	全局配置模式	使能某个接口的 loopdetection 功能
no loop-detection *slot-list/port-list*	全局配置模式	关闭某个接口的 loopdetection 功能

参数说明：

slot-list/port-list：格式如：1/5-10,17,19。

15.2.2. loopdetection keepalive

配置 loopdetection 功能发送 keeplive 报文的时间间隔，默认为 30s。

表 15–2 配置 loopdetection keepalive 间隔时间

命令	命令模式	功能说明
loop-detectioin interval-timer *time_value*	全局配置模式	配置 loopdetection 功能发送 keeplive 报文的时间间隔
no loop-detectioin interval-timer *time_value*	全局配置模式	恢复 keepalive 间隔时间为默认值 30s

参数说明：

time_value ：Keepalive 间隔时间，默认为 30s，范围<5,300>。

15.2.3. Loopdetection 可控制 shutdown

表 15–3 Loopdetection 可控制 shutdown

命令	命令模式	功能说明
loop-detection control enable *slot-list/port-list*	全局配置模式	开启/关闭 loopdetection 可控制 shutdown 功能。
no loop-detection control enable *slot-list/port-list*	全局配置模式	开启/关闭 loopdetection 可控制 shutdown 功能。

参数说明：

slot-list/port-list 格式如：1/5-10,17,19。

15.2.4. Loopdetection 消息老化时间

表 15–4 配置 Loopdetection 消息老化时间

命令	命令模式	功能说明
loop-detection message age-timer *time_value*	全局配置模式	配置消息老化时间
no loop-detection message age-timer	全局配置模式	恢复消息老化时间为默认值

参数说明

time_value : 消息老化时间，默认为 60s，范围<5,300>

15.2.5. loopdetection 的监控与维护

表 15–5 loopdetection 的监控与维护

命令	命令模式	功能说明
debug switch loop-detection {all | error | dbg | rx | tx}	特权用户模式	调试 loopdetection 功能。
no debug switch loop-detection {all |	特权用户模式	关闭 debug 模式。

error | dbg | rx | tx}		
show loop-detection	特权用户模式	查看 loopdetection 的接口信息。
show loop-detection msg *slot/port*	特权用户模式	查看指定接口下 loop-detection 功能的参数信息

参数说明：

group-id：TURNK 组的 ID，范围为 1-4。

第 16 章 IP、MAC 绑定

16.1. Ip mac bind 简介

使能该功能后，默认禁止所有报文通过，只有匹配 ip mac bind 关系的报文才能通过。

16.2. Ip mac bind 配置

16.2.1. 使能/关闭 ip mac bind

使能/关闭 ip mac bind 功能。

表 16–1 使能/关闭 ip mac bind 功能

命令	命令模式	功能说明
ip-bind-mac enable	全局配置模式	使能 ip mac bind 功能
ip-bind-mac disable	全局配置模式	关闭 ip mac bind 功能

16.2.2. 配置 ip mac bind 关系

表 16–2 配置 ip mac bind 关系

命令	命令模式	功能说明
ip *src_ip* **bind mac {***src_mac* | **any} [port** s*lot-list/port-list***]**	全局配置模式	配置 ip mac bind 关系
no ip *src_ip* **bind mac {***src_mac* | **any} [port** s*lot-list/port-list***]**	全局配置模式	删除 ip mac bind 关系

参数说明：

src_ip：源 ip 地址，0.0.0.0 表示任意 ip。

src_mac：源 mac 地址。any 表示任意 mac 地址。

slot-list/port-list：格式如：1/5-10,17,19

16.2.3. 查看 ip mac bind 关系及状态

表 169–3 查看 ip mac bind 关系及状态

命令	命令模式	功能说明
show ip mac bind	特权配置模式	查看 ip mac bind 关系及状态